The Open University

M303

Further pure mathematics

Book E

Rings and fields

This publication forms part of the Open University module M303 *Further pure mathematics*. Details of this and other Open University modules can be obtained from Student Recruitment, The Open University, PO Box 197, Milton Keynes MK7 6BJ, United Kingdom (tel. +44 (0)300 303 5303; email general-enquiries@open.ac.uk).

Alternatively, you may visit the Open University website at www.open.ac.uk where you can learn more about the wide range of modules and packs offered at all levels by The Open University.

The Open University, Walton Hall, Milton Keynes, MK7 6AA.

First published 2014. Second edition 2016.

Copyright © 2014, 2016 The Open University

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, transmitted or utilised in any form or by any means, electronic, mechanical, photocopying, recording or otherwise, without written permission from the publisher or a licence from the Copyright Licensing Agency Ltd. Details of such licences (for reprographic reproduction) may be obtained from the Copyright Licensing Agency Ltd, Saffron House, 6–10 Kirby Street, London EC1N 8TS (website www.cla.co.uk).

Open University materials may also be made available in electronic formats for use by students of the University. All rights, including copyright and related rights and database rights, in electronic materials and their contents are owned by or licensed to The Open University, or otherwise used by The Open University as permitted by applicable law.

In using electronic materials and their contents you agree that your use will be solely for the purposes of following an Open University course of study or otherwise as licensed by The Open University or its assigns.

Except as permitted above you undertake not to copy, store in any medium (including electronic storage or use in a website), distribute, transmit or retransmit, broadcast, modify or show in public such electronic materials in whole or in part without the prior written consent of The Open University or in accordance with the Copyright, Designs and Patents Act 1988.

Edited, designed and typeset by The Open University, using the Open University TEX System.

Printed in the United Kingdom by Halstan & Co. Ltd, Amersham, Bucks.

ISBN 978 1 4730 2040 5

2.1

Contents

Chapter 17 Rings and homomorphisms **1**

Introduction **3**

1 Fields of fractions **5**
1.1 The field of fractions of an integral domain 5
1.2 Polynomial rings over a UFD 15

2 Ideals **21**
2.1 Ideals and their properties 21
2.2 Principal ideal domains 27

3 Operations on ideals **34**
3.1 Sum of ideals 34
3.2 Product of ideals 35
3.3 Finitely generated ideals 37

4 Quotients **40**
4.1 Cosets of an ideal 40
4.2 Homomorphisms 45
4.3 The First Isomorphism Theorem 49
4.4 Quotient rings of $K[x]$ 51
4.5 Prime ideals 55

Learning outcomes **58**

Solutions to exercises **59**

Chapter 18 Fields and polynomials **71**

Introduction **73**

1 Preliminaries **74**
1.1 Isomorphisms and homomorphisms between fields 74
1.2 Characteristic of a field 82

2 Field extensions **85**
2.1 Vector spaces 86
2.2 Extensions of fields by elements 91
2.3 Algebraic extensions 93
2.4 Transcendental extensions 105

3 Finite fields **107**
3.1 The multiplicative group of a finite field 107
3.2 Roots and inverses in the multiplicative group 111

4 Splitting fields **115**
4.1 Existence and uniqueness of splitting fields 115
4.2 Existence and uniqueness of finite fields 122

Learning outcomes **128**

Solutions to exercises **129**

Chapter 19 Fields and geometry **137**

Introduction **139**

1 Field extensions revisited **141**
1.1 Algebraic extensions revisited 143
1.2 The field of algebraic numbers 145
1.3 Transcendental extensions revisited 150

2 Ruler and compasses constructions **155**
2.1 Geometric constructions 155
2.2 Ruler and compasses algebraically 158
2.3 Coordinates and field extensions 163
2.4 Impossibility proofs for classical Greek problems 168
2.5 Constructible complex numbers 170

Learning outcomes **172**

Solutions to exercises **173**

Chapter 20 Public-key cryptography **185**

Introduction **187**

1 Cryptosystems based on modular arithmetic **189**
1.1 Algebraic preliminaries 189
1.2 The RSA cryptosystem 199
1.3 Examples of RSA cryptosystems 201
1.4 How secure are RSA cryptosystems? 204
1.5 The Diffie–Hellman cryptosystem 209

2 Cryptosystems based on elliptic curves **212**
2.1 First things first: cubic polynomials 212
2.2 Elliptic curves: definition and examples 215
2.3 Elliptic curves as abelian groups 221
2.4 Examples of elliptic curves as abelian groups 229
2.5 Two cryptosystems based on elliptic curves 234

Learning outcomes **242**

Solutions to exercises **243**

Index **251**

Chapter 17

Rings and homomorphisms

Introduction

As you saw in Book C, Chapter 11, a ring can be thought of as a collection of objects that we can add, subtract and multiply, but not necessarily divide. There are many mathematical structures where this is precisely what we can do. The simplest and most familiar of these structures arises from the integers, where dividing one integer by another does not always give a third integer. From a mathematical point of view, the principal benefit we get from this constraint is the rich theory of prime numbers and the factorisation of integers in an essentially unique way into a product of primes.

Other mathematical structures where division is not closed include the rings of polynomials in one or several variables. Here the coefficients of the polynomials come themselves from a ring. They might, for example, be required to be integers, or they might belong to the field of real numbers. Polynomials are important in mathematics, and an interesting question is to what extent a ring of polynomials resembles the familiar ring of integers.

Of course, not being able to divide can be irksome, and in the case of the integers we can construct the smallest collection of objects that allows us to divide any integer by any (non-zero) integer. Such a quotient will not generally be an integer: it will be what we call a *rational number*. The collection of all the numbers obtained in this way forms the field of rational numbers. These numbers can be added, subtracted, multiplied and divided.

You may be familiar with the stories we tell children when introducing them to the rational numbers, in which they share out slices of pizzas and cakes, and which can leave them unsure why dividing by $\frac{1}{2}$, for example, has the same effect as multiplying by 2. Here we present a mathematical construction of the rationals that explains this informal notion of division much more systematically. Moreover, it can be applied to any integral domain, yielding a field that contains the integral domain and all the quotients of the elements of the integral domain. This field is called the *field of fractions* of the integral domain.

When dealing with polynomial rings where the coefficient ring is arbitrary, it is natural to wonder if the polynomials behave more or less as they do when the coefficients are integers. For example, can we factorise a polynomial as a product of irreducible polynomials, and can we do so in an essentially unique way? If the answer is 'yes', then this is one way in which the polynomial ring resembles the ring of integers. In fact, the answer depends on the ring of coefficients: if the ring of coefficient R is a unique factorisation domain then, as you will see, the polynomial ring $R[x]$ is also a unique factorisation domain. The proof is interesting because it makes use of F, the field of fractions of R, and allows us to compare the irreducibility of a polynomial in $R[x]$ with the same polynomial as an element of $F[x]$.

After working with polynomial rings, we consider rings more generally. Rings are, in particular, groups with a binary operation $+$, and we can look for objects and theorems in our theory of rings that resemble those that we find in group theory. A key notion is that of an *ideal*. In ring theory, ideals play a similar role to normal subgroups in group theory. As for groups, the ring of integers is a good source of examples: every non-trivial ideal in this ring consists of the multiples of a single positive integer. For example, the set of all multiples of 6 is an ideal in $\mathbb{Z}$. The notion of ideal is closely related to that of divisibility: for example, the ideal of all multiples of 3 in $\mathbb{Z}$ contains the ideal of all multiples of 6 in $\mathbb{Z}$, because every multiple of 6 is also a multiple of 3. In rings in which every ideal consists of multiples of a single element, the so-called *principal ideal rings*, there is a good theory of highest common divisors and least common multiples.

Like subgroups of a group, ideals of a ring can be used to construct other ideals. For example, we can form sums and products of ideals. Moreover, ideals arise as the kernels of ring homomorphisms, and there are analogues of the key isomorphism theorems in group theory. But perhaps the most important fact about ideals is that they give rise to new rings as quotients of a ring by one of its ideals, in the same way as normal subgroups give rise to quotient groups in group theory. In the example of the ideal of all multiples of 6 in $\mathbb{Z}$, the quotient ring is the ring of integers modulo 6.

An even richer example is a certain construction of the complex numbers from $\mathbb{R}$, the ring of real numbers. In this construction, we first build the polynomial ring $\mathbb{R}[x]$, then we construct the ideal I of all multiples of the polynomial $x^2 + 1$ by elements of $\mathbb{R}[x]$. Finally, we quotient $\mathbb{R}[x]$ by I. As you will see in Section 4.4, the resulting ring is isomorphic to the ring of complex numbers.

There are two properties of a prime number that you met in the wider context of rings in Book C, Chapter 12, Section 2.2. The first is irreducibility: a number is irreducible if it cannot be factored as a product in a non-trivial way. The second is primality: a number p is prime if whenever it divides a product ab it divides one of the factors – either p divides a or p divides b. As you saw in Book C, Chapter 13, in a general ring it can happen that an element is irreducible but does not have the second property. The way to pursue the analogy with the integers is to introduce the notion of *prime* ideal, so the chapter concludes with a study of prime ideals.

Chapter guide

Although Section 4 is substantially longer than the other sections, much of the material is very closely related to the material on quotient groups that was covered in Book B. Section 4 requires about twice as much study time as Section 1. Sections 2 and 3 together require about the same amount of study time as Section 1.

1 Fields of fractions

In this section we will introduce the field of fractions of an integral domain. This field is obtained by expanding the integral domain to a larger ring in which all non-zero elements have multiplicative inverses. For example, consider the relationship between the ring $\mathbb{Z}$ of integers and the field $\mathbb{Q}$ of rational numbers. We know that $\mathbb{Z} \subset \mathbb{Q}$, and that all non-zero elements in $\mathbb{Q}$ have multiplicative inverses. The inclusion $\mathbb{Z} \subset \mathbb{Q}$ is often called an *embedding*, and we say that the ring of integers is *embedded* into the field of rational numbers. The elements of $\mathbb{Q}$, that is, the rational numbers, are fractions formed by the integers. This way of looking at $\mathbb{Z}$ and $\mathbb{Q}$ leads to a far-reaching generalisation, which is the construction of a field of fractions from an integral domain. This construction has an important application to polynomial rings over unique factorisation domains.

1.1 The field of fractions of an integral domain

Let us start by recalling how the rational numbers are constructed from the integers. We know that, for example, $\frac{2}{3}$ and $\frac{6}{9}$ represent the same rational number. More generally, two fractions $\frac{a}{b}$ and $\frac{c}{d}$ represent the same rational number if, and only if, $ad = bc$. So a rational number can be thought of as an infinite set of fractions $\frac{a}{b}$, each of which represents the number.

In mathematically rigorous terms, what we do is introduce an equivalence relation on the set of ordered pairs

$$\{(a, b) : a, b \in \mathbb{Z}, b \neq 0\}$$

by stipulating that two pairs (a, b) and (c, d) are equivalent if $ad = bc$. A rational number is defined as an equivalence class under this relation. We then introduce addition and multiplication of rational numbers in the usual way and prove that the two operations are well defined, that is, they do not depend on the choice of ordered pairs representing the rational numbers.

In what follows, we mimic this construction of the rational numbers from the integers, but instead of the integers we start off with a general integral domain.

Recall from Book C, Chapter 12, Definition 2.8 that $(D, +, \cdot)$ is an integral domain if it is a commutative ring with unity and with no zero divisors. As in Book C, throughout this book we usually simplify notation by using juxtaposition rather than $\cdot$ for the second ring operation.

Now let S_D be the set of all ordered pairs (a, b) of elements of D such that $b \neq 0$, that is

$$S_D = \{(a, b) : a, b \in D,\ b \neq 0\}.$$

We introduce a binary relation $\sim$ on the set S_D as follows:

$$(a, b) \sim (c, d) \text{ if, and only if, } ad = bc.$$

Our aim is to show that $\sim$ is an equivalence relation, namely that it is reflexive, symmetric and transitive.

Exercise 1.1

Let $(D, +, \cdot)$ be an integral domain and let

$$S_D = \{(a, b) : a, b \in D,\ b \neq 0\}.$$

Show that the relation $\sim$ on the set S_D defined by

$$(a, b) \sim (c, d) \text{ if, and only if, } ad = bc$$

is reflexive and symmetric.

Proposition 1.1

Let $(D, +, \cdot)$ be an integral domain and let

$$S_D = \{(a, b) : a, b \in D,\ b \neq 0\}.$$

Then the relation $\sim$ on the set S_D defined by

$$(a, b) \sim (c, d) \text{ if, and only if, } ad = bc$$

is an equivalence relation.

Proof We proved that the relation is symmetric and reflexive in the solution to Exercise 1.1, so we just need to show transitivity. Let (a, b), (c, d) and (e, f) be elements of S_D such that $(a, b) \sim (c, d)$ and $(c, d) \sim (e, f)$. To prove that $\sim$ is transitive we need to show that $(a, b) \sim (e, f)$.

Since $(a, b) \sim (c, d)$, we have that $ad = bc$. Multiplying both sides of this equality on the right by f gives

$$adf = bcf.$$

Similarly, $(c, d) \sim (e, f)$ gives $cf = de$, and left multiplication by b gives

$$bcf = bde.$$

Therefore $adf = bde$, and so $afd = bed$ since multiplication is commutative in D. Since D is an integral domain, $af = be$ by cancellation (Book C, Chapter 12, Lemma 2.11). Thus $(a, b) \sim (e, f)$ as required. ■

We now know that $\sim$ is an equivalence relation, and so we let F_D denote the set of equivalence classes on S_D induced by $\sim$, that is,

$$F_D = S_D/\sim .$$

For any $(a, b) \in S_D$, the equivalence class in F_D containing the element (a, b) is denoted by $[a, b]$:

$$[a, b] = \{(c, d) \in S_D :\ (a, b) \sim (c, d)\}.$$

On this new set F_D we introduce the operations of addition $+$ and multiplication $\cdot$ as follows:

$$[a,b]+[c,d]=[ad+bc,bd]$$
$$[a,b]\cdot[c,d]=[ac,bd].$$

We will again simplify notation by using juxtaposition in place of $\cdot$ for multiplication.

Our next aim is to show that these two operations are well defined, that is, independent of the choice of representatives for equivalence classes.

As regards addition, we have to show that if $[a,b]=[a_1,b_1]$ and $[c,d]=[c_1,d_1]$, then $[ad+bc,bd]=[a_1d_1+b_1c_1,b_1d_1]$.

Our assumptions say that $(a,b)\sim(a_1,b_1)$ and $(c,d)\sim(c_1,d_1)$, which implies that

$$ab_1=ba_1 \text{ and } cd_1=c_1d \qquad (*)$$

and we would like to conclude that $(ad+bc,bd)\sim(a_1d_1+b_1c_1,b_1d_1)$. That is, we would like to prove

$$(ad+bc)(b_1d_1)=(bd)(a_1d_1+b_1c_1).$$

Since D is an integral domain, $bd\neq 0$, so both operations are closed in S_D.

Now

$$\begin{aligned}(ad+bc)(b_1d_1)&=adb_1d_1+bcb_1d_1\\&=ab_1dd_1+bb_1cd_1\\&=ba_1dd_1+bb_1c_1d \quad \text{by } (*)\\&=bda_1d_1+bdb_1c_1\\&=(bd)(a_1d_1+b_1c_1),\end{aligned}$$

as required.

The next exercise asks you to check that multiplication is well defined.

Exercise 1.2

Using the notation just given, show that $[a,b][c,d]=[ac,bd]$ is well defined, that is, it is independent of the choice of equivalence classes.

We now want to show that the algebraic structure $(F_D,+,\cdot)$ is a field, that is, a commutative ring with unity where every non-zero element has a multiplicative inverse (see Book C, Chapter 11, Definition 1.14). In order to do this, we start by showing that cancellation holds with these operations, and we describe the equivalence class of $(0,1)$, which will be the additive identity.

Lemma 1.2

Let D be an integral domain and let $S_D = \{(a, b) : a, b \in D,\ b \neq 0\}$. Let $F_D = \{[a, b] : (a, b) \in S_D\}$ denote the set of equivalence classes on S_D induced by the relation $\sim$ defined by

$$(a, b) \sim (c, d) \text{ if, and only if, } ad = bc.$$

(a) If $a, b, c \in D$ with $b \neq 0$ and $c \neq 0$, then $(a, b) \sim (ac, bc)$.

(b) If $a, b, d \in D$ with $b \neq 0$ and $d \neq 0$, then $(a, b) \sim (0, d)$ if, and only if, $a = 0$.

Proof

(a) Since D is commutative, $abc = bac$ for all a, b and c in D. This implies that $(a, b) \sim (ac, bc)$.

(b) We have $(a, b) \sim (0, d)$ if, and only if, $ad = b0 = 0$. Since D has no zero divisors and $d \neq 0$, $ad = 0$ if, and only if, $a = 0$.

Therefore $(a, b) \sim (0, d)$ if, and only if, $a = 0$, as required. ■

Proposition 1.3

Let D be an integral domain and let S_D and F_D be as in Lemma 1.2. Let $+$ and $\cdot$ be binary operations on F_D defined by

$$[a, b] + [c, d] = [ad + bc, bd]$$
$$[a, b] \cdot [c, d] = [ac, bd].$$

Then F_D is a field with the property that every element can be written in the form

$$[a, 1][b, 1]^{-1}$$

for some $a, b \in D$, $b \neq 0$.

Proof We know from the solution to Exercise 1.2 and the discussion preceding it that the two binary operations $+$ and $\cdot$ are well defined. We now check the axioms for a field given in Definitions 1.1 and 1.14 of Book C, Chapter 11.

Axioms for addition

R1 Closure For all $[a,b],[c,d] \in F_D$, we have that $bd \neq 0$ because $b \neq 0$ and $d \neq 0$, and D has no zero divisors. Therefore

$$[a,b]+[c,d] = [ad+bc, bd] \in F_D.$$

R2 Associativity For all $[a,b],[c,d],[e,f] \in F_D$,

$$\begin{aligned}[a,b]+([c,d]+[e,f]) &= [a,b]+[cf+de, df] \\ &= [adf+b(cf+de), bdf] \\ &= [adf+bcf+bde, bdf] \\ &= [(ad+bc)f+bde, bdf] \\ &= [ad+bc, bd]+[e,f] \\ &= ([a,b]+[c,d])+[e,f].\end{aligned}$$

Note that this argument uses both associativity and distributivity in D.

R3 Additive identity For all $[a,b] \in F_D$,

$$[a,b]+[0,1] = [a,b] = [0,1]+[a,b].$$

R4 Additive inverses For each $[a,b] \in F_D$,

$$[a,b]+[-a,b] = [0,1] = [-a,b]+[a,b].$$

R5 Commutativity For all $[a,b],[c,d] \in F_D$,

$$\begin{aligned}[a,b]+[c,d] &= [ad+bc, bd] \\ &= [cb+da, db] \text{ from the commutativity of } D \\ &= [c,d]+[a,b].\end{aligned}$$

Axioms for multiplication

R6 Closure For all $[a,b],[c,d] \in F_D$,

$$[a,b][c,d] = [ac, bd] \in F_D \text{ since } b \neq 0 \text{ and } d \neq 0.$$

As in the proof of additive closure, here we are using the fact that D has no zero divisors, which is true because D is an integral domain.

R7 Associativity For all $[a,b],[c,d],[e,f] \in F_D$,

$$\begin{aligned}[a,b]([c,d][e,f]) &= [a,b][ce, df] \\ &= [ace, bdf] \\ &= [ac, bd][e,f] \\ &= ([a,b][c,d])[e,f].\end{aligned}$$

This argument uses associativity in D.

R8 Multiplicative identity For all $[a,b] \in F_D$,

$$[a,b][1,1] = [a,b] = [1,1][a,b].$$

Axioms combining addition and multiplication

R9 Distributive laws For all $[a,b],[c,d],[e,f] \in F_D$,

$$\begin{aligned}
[a,b]([c,d]+[e,f]) &= [a,b][cf+de,df] \\
&= [acf+ade,bdf]. \\
([a,b][c,d])+([a,b][e,f]) &= [ac,bd]+[ae,bf] \\
&= [acbf+bdae,bdbf] \\
&= [acf+dae,bdf] \text{ using Lemma 1.2(a)} \\
&= [acf+ade,bdf] \text{ by the commutativity of } D.
\end{aligned}$$

This shows that the left distributive law holds. The right distributive law follows from left distributivity by the commutativity of D.

We are now left to check axioms R10 and R11.

R10 Commutativity For all $[a,b],[c,d] \in F_D$,

$$[a,b][c,d] = [ac,bd] = [ca,db] = [c,d][a,b] \text{ by the commutativity of } D.$$

R11 Multiplicative inverses Let $[a,b]$ be a non-zero element of F_D. Then Lemma 1.2(b) implies that $a \neq 0$, so $[b,a] \in F_D$. Moreover,

$$\begin{aligned}
[a,b][b,a] &= [ab,ba] = [1,1] \quad \text{and} \\
[b,a][a,b] &= [ba,ab] = [1,1]
\end{aligned}$$

by Lemma 1.2(a). Thus $[b,a]$ is the multiplicative inverse of $[a,b]$, that is $[b,a] = [a,b]^{-1}$.

Thus, all the field axioms hold in F_D. Now let $[a,b] \in F_D$. Then

$$[a,b] = [a,1][1,b] = [a,1][b,1]^{-1},$$

and so every element of F_D has the required form. ■

We are used to thinking of the integers as a subring of the rationals by identifying the integer a with the rational $\frac{a}{1}$. In terms of the equivalence relation that we defined on $\{(a,b) : a,b \in \mathbb{Z}, b \neq 0\}$, we identify the elements of $\mathbb{Z}$ with the elements of the set $\{[a,1] : a \in \mathbb{Z}\}$.

Similarly, in the general case the set

$$\{[a,1] \in F_D : a \in D\}$$

is a copy of D in F_D, and, just as with rational numbers, we identify the elements of this set with the elements of D. Now, we know from Proposition 1.3 that every element $[a,b]$ of F_D can be written as $[a,1][b,1]^{-1}$. So we can extend our identification to the whole of F_D by thinking of $[a,b] \in F_D$ as ab^{-1}, where a and $b \in D$ and $b \neq 0$.

This identification is the defining feature of a field of fractions, and it can be expressed in rigorous mathematical terms using the notion of a *ring isomorphism*.

Definition 1.4 *Ring isomorphism*

Let R and S be rings. Then we say that R and S are **isomorphic** if there is a bijection $\theta : R \to S$ such that, for all $a, b \in R$,

- $\theta(a + b) = \theta(a) + \theta(b)$
- $\theta(ab) = \theta(a)\theta(b)$
- $\theta(1_R) = 1_S$.

The bijection θ is said to be a **ring isomorphism**.

We often refer to the properties of addition and multiplication in Definition 1.4 as the **homomorphism** or **morphism properties**.

With this definition we can now check that for a given integral domain D the field of fractions F_D is unique up to isomorphism.

Proposition 1.5

Let E be a field, and let D be a subring of E such that

1. D is an integral domain
2. every element of E can be written as ab^{-1} with $a, b \in D$.

Then E is isomorphic to F_D.

Proof We show that the map

$$\begin{aligned} \theta : \quad E &\to F_D \\ ab^{-1} &\mapsto [a, b] \end{aligned}$$

is an isomorphism. Let ab^{-1} and $cd^{-1} \in E$. Then

$$\begin{aligned} ab^{-1} + cd^{-1} &= add^{-1}b^{-1} + cbb^{-1}d^{-1} \\ &= ad(bd)^{-1} + bc(bd)^{-1} \\ &= (ad + bc)(bd)^{-1}. \end{aligned}$$

This calculation makes use of the associative, commutative and distributive laws in E. We use this equality to check that θ satisfies the properties in Definition 1.4. Remember that $[1, 1]$ is the multiplicative identity of F_D.

- $$\begin{aligned} \theta(ab^{-1} + cd^{-1}) &= \theta((ad + bc)(bd)^{-1}) \\ &= [ad + bc, bd] \\ &= [a, b] + [c, d] \end{aligned}$$
- $$\begin{aligned} \theta(ab^{-1}cd^{-1}) &= \theta(ac(bd)^{-1}) \\ &= [ac, bd] \\ &= [a, b][c, d] \end{aligned}$$
- $$\begin{aligned} \theta(1) &= \theta(1 \cdot 1^{-1}) \\ &= [1, 1] \end{aligned}$$

We have to show that θ is a bijection. Since any $[a, b] \in F_D$ is the image of $ab^{-1} \in E$, θ is onto.

Moreover, $\theta(ab^{-1}) = \theta(cd^{-1}) \implies [a, b] = [c, d]$
$\implies ad = bc$
$\implies ab^{-1} = cd^{-1}$,
which shows that θ is one–one.

Thus θ is a bijection, and so it is a ring isomorphism. ■

Proposition 1.5 ensures that an integral domain has a unique field of fractions up to isomorphism, so the following definition is justified.

Definition 1.6 *Field of fractions*

Let D be an integral domain. Then a field F_D is called the **field of fractions** of D if D is isomorphic to a subring A of F_D and every element of F_D can be written as ab^{-1} where $a, b \in A$ and $b \neq 0$.

The isomorphism whose existence we proved in Proposition 1.5 allows us to use the definite article 'the' before 'field of fractions'.

In the preceding discussion we have used the notation $[a, b]$ for the equivalence class corresponding to an element of F_D. It is, however, usual to adopt the fraction notation $\frac{a}{b}$, and we will do this from now on.

We will also stop using the notation F_D and simply refer to F as the field of fractions of an integral domain D.

Example 1.7 *Two fields of fractions*

(a) Let $\mathbb{Z}$ denote the ring of integers. The field of rational numbers $\mathbb{Q}$ is isomorphic to the field of fractions F of the integers.

(b) The field of *rational functions*, which has underlying set

$$\left\{ \frac{f(x)}{g(x)} : f(x), g(x) \in \mathbb{Q}[x], g(x) \neq 0 \right\},$$

is the field of fractions of $\mathbb{Q}[x]$. It is often denoted by $\mathbb{Q}(x)$.

Worked Exercise 1.8

Worked Exercise 1.9 of Book C, Chapter 11 introduced the ring of Gaussian integers

$$\mathbb{Z}[i] = \{a + ib : a, b \in \mathbb{Z}\}.$$

What is the field of fractions of $\mathbb{Z}[i]$?

Solution

By the remark immediately preceding Example 1.7, we may identify the elements of the field of fractions of the Gaussian integers with fractions of the form

$$\frac{a+bi}{c+di},$$

where $a, b, c, d \in \mathbb{Z}$ and c, d are not both equal to 0, so that $c + id \neq 0$.

If we consider the fractions with $d = 0$, we see that the field of fractions contains all the elements of the form $a_1 + b_1 i$, where $a_1, b_1 \in \mathbb{Q}$. On the other hand, multiplying the numerator and the denominator of $\frac{a+bi}{c+di}$ by $c - di$ gives

$$\frac{(a+bi)(c-di)}{(c+di)(c-di)} = \frac{ac+bd+i(bc-ad)}{c^2+d^2} = \frac{ac+bd}{c^2+d^2} + i\left(\frac{bc-ad}{c^2+d^2}\right).$$

This shows that these fractions always have the form $a_1 + b_1 i$ where $a_1, b_1 \in \mathbb{Q}$.

We conclude that the field of fractions of the Gaussian integers $\mathbb{Z}[i]$ is isomorphic to

$$\mathbb{Q}[i] = \{a + bi : a, b \in \mathbb{Q}\},$$

which is known as the **field of Gaussian numbers**.

Alternatively, we can show that $\mathbb{Q}[i]$ is the field of fractions for $\mathbb{Z}[i]$ by proving that $\mathbb{Q}[i]$ is a field and that every element can be written in the form ab^{-1} where $a, b \in \mathbb{Z}[i]$.

We leave you to check that $\mathbb{Q}[i]$ is an integral domain. Then, in order to show that $\mathbb{Q}[i]$ is a field, we just need to show that every non-zero element has a multiplicative inverse.

Let $a + bi \in \mathbb{Q}[i]$ be such that $a + bi \neq 0$, so that $a^2 + b^2 \neq 0$. Then

$$(a+bi)\left(\frac{a}{a^2+b^2} - \frac{b}{a^2+b^2}i\right) = \frac{(a+ib)(a-ib)}{a^2+b^2} = 1.$$

Thus we have shown that every non-zero element $a + bi$ of $\mathbb{Q}[i]$ has a multiplicative inverse in $\mathbb{Q}[i]$. Therefore $\mathbb{Q}[i]$ is a field.

Now let $a + bi \in \mathbb{Q}[i]$ with $a = \frac{a_1}{a_2}$, $b = \frac{b_1}{b_2}$ where $a_1, a_2, b_1, b_2 \in \mathbb{Z}$ and $a_2 \neq 0$, $b_2 \neq 0$. Then

$$a + bi = \frac{a_1}{a_2} + \frac{b_1}{b_2}\, i = \frac{a_1 b_2 + b_1 a_2 i}{a_2 b_2} = (a_1 b_2 + b_1 a_2 i)(a_2 b_2)^{-1}.$$

Thus we can write every element of $\mathbb{Q}[i]$ in the form cd^{-1} where $c, d \in \mathbb{Z}[i]$. Hence $\mathbb{Q}[i]$ is the field of fractions of $\mathbb{Z}[i]$ by Definition 1.6.

Exercise 1.3

(a) Show that there exist $f \in \mathbb{Q}$, and $p(x) \in \mathbb{Z}[x]$ such that

$$\frac{1}{2} + \frac{2}{3}x + \frac{1}{5}x^3 = fp(x).$$

(b) Let $R[x]$ be a polynomial ring over an integral domain R and let F be the field of fractions of R. Show every element $q(x) \in F[x]$ can be written as $fp(x)$ where $f \in F$ and $p(x) \in R[x]$.

Using the fraction notation might make you wonder whether we can always write the elements of a field of fractions as fractions in their 'lowest terms', in some sense of 'lowest'. In the next exercise you are asked to show that this can be done when D is a unique factorisation domain, or UFD – recall Definition 4.1 of Book C, Chapter 12.

Exercise 1.4

Let D be a UFD and let F be the field of fractions of D. Let $\frac{a}{b} \in F$ be a non-zero element, so that $a \neq 0$. Show that there exist $c, d \in D$ such that

$$\frac{a}{b} = \frac{c}{d}$$

and $\text{hcf}(c, d) = u$, where u is a unit in D.

When two elements c and d of a unique factorisation domain D are such that $\text{hcf}(c, d)$ is a unit, we say that $\frac{c}{d} \in F_D$ is a **fraction in its lowest terms**.

Exercise 1.5

Let D be a UFD and let F be the field of fractions of D. Let S be a finite set of fractions,

$$S = \left\{ \frac{a_i}{b_i} : a_i, b_i \in D,\ b_i \neq 0,\ i = 1, \ldots, n \right\}.$$

(a) Show that there is $b \in D$ such that

(i) $b = b_i c_i$ for some c_i, $i = 1, \ldots, n$;

(ii) if $d = b_i d_i$ for some d_i, $i = 1, \ldots, n$ then $d = bc$ for some $c \in D$.

That is, show that $\text{lcm}(b_1, b_2, \ldots, b_n)$ exists.

(b) Let $\frac{a_i}{b_i} \in S$. Show that $\frac{a_i}{b_i} = \frac{a_i c_i}{b}$.

Hint: for part (a), use the result in Exercise 4.1 in Book C, Chapter 12.

The element $b \in D$ in Exercise 1.5 is known as a **lowest common denominator** of the set of fractions S.

1.2 Polynomial rings over a UFD

In Theorem 4.11 of Book C, Chapter 12, we proved that $\mathbb{Z}[x]$ is a UFD. A key step in the proof is to consider a polynomial in $\mathbb{Z}[x]$ as a polynomial in $\mathbb{Q}[x]$ in order to use the fact that $\mathbb{Q}[x]$ is a Euclidean domain. Any UFD is an integral domain and so it has a field of fractions. This means we can generalise this key step to any UFD to prove the main theorem of this subsection, namely that if R is a UFD then $R[x]$ is a UFD. We start by generalising some definitions and Gauss's Lemma (Theorem 4.13 of Book C, Chapter 11), which is the key preliminary result linking factorisation in $\mathbb{Z}[x]$ with factorisation in $\mathbb{Q}[x]$.

Definition 1.9 *Primitive polynomial*

Let R be a unique factorisation domain, and let

$$f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$$

be a polynomial in $R[x]$.

(a) The **content** of f is a highest common factor of all of its coefficients in R:

$$c_f = \text{hcf}(a_0, a_1, \ldots, a_n).$$

(b) $f(x)$ is **primitive** if $c_f = u$ for some unit in $u \in R$. In other words, $f(x)$ is primitive if the only common factors of its coefficients are units of R.

In general, highest common factors in a UFD are only unique up to multiplication by a unit, so the same is true of the content. This is why we define the content as 'a' highest common factor of the coefficients (rather than 'the' highest common factor).

As a consequence of Definition 1.9, if R is a unique factorisation domain and $f(x) \in R[x]$, we can write $f(x) = c_f g(x)$ where $g(x)$ is a primitive polynomial in $R[x]$.

The following lemma is the natural extension to UFDs of Lemma 4.12 of Book C, Chapter 11.

Lemma 1.10

Let R be a unique factorisation domain. Then f and g are primitive polynomials in $R[x]$ if, and only if, their product fg is primitive.

Proof The proof is the same as that of Lemma 4.12 of Book C, Chapter 11 with $\mathbb{Z}$ replaced by R and with $p \in \mathbb{Z}$ replaced by an irreducible element $r \in R$. ■

Lemma 1.10 enables us to prove a generalised version of Gauss's Lemma. The proof is very similar to that of Theorem 4.13 in Chapter 11, but we will repeat it here, as the general case uses the field of fractions of a UFD.

Lemma 1.11 *Gauss's Lemma for UFDs*

Let R be a UFD and let F be the field of fractions of R. Let $f(x)$ be a primitive polynomial in $R[x]$. If we can write $f = gh$ with $g, h \in F[x]$, then we can write $f = GH$ with $G, H \in R[x], \deg(g) = \deg(G)$ and $\deg(h) = \deg(H)$.

Proof Since $g(x)$ is a polynomial in $F[x]$, by the solution to Exercise 1.5 we can find a lowest common denominator, b say, of all its coefficients. Then we can write $g(x) = \frac{a}{b}\hat{G}(x)$, where $\hat{G}(x)$ is a primitive polynomial and we may assume that $\frac{a}{b}$ is a fraction in its lowest terms by the solution to Exercise 1.4.

Similarly we can write $h(x) = \frac{c}{d}\hat{H}(x)$ where $\hat{H}(x)$ is a primitive polynomial in $R[x]$ and $\frac{c}{d}$ is a fraction in lowest terms. Note that $\deg(g) = \deg(\hat{G})$ and $\deg(h) = \deg(\hat{H})$. Hence

$$f(x) = g(x)h(x) = \frac{ac}{bd}\hat{G}(x)\hat{H}(x).$$

We now prove that $f = u\hat{G}\hat{H}$ for some unit $u \in R$, and so we need to show that $ac = ubd$. Rearranging, we find that $bdf = ac\hat{G}\hat{H}$. Since f is primitive, the content of $bdf(x)$ is bd. Moreover, by Lemma 1.10, $\hat{G}\hat{H}$ is primitive, and so the content of $ac\hat{G}(x)\hat{H}(x)$ is ac. Since the polynomials $bdf(x)$ and $ac\hat{G}(x)\hat{H}(x)$ are equal, so must their contents be equal, and hence $ac = ubd$ for some unit $u \in R$ as required.

Taking $G = u\hat{G}$ and $H = \hat{H}$ gives the required factorisation $f = GH$. ■

We are almost ready to prove that a polynomial ring over a UFD is itself a UFD. The proof that $\mathbb{Z}[x]$ is a UFD given in Book C, Chapter 12, Subsection 4.2 used the following steps:

1. Every polynomial in $\mathbb{Z}[x]$ has a factorisation into irreducible polynomials in $\mathbb{Z}[x]$ (Lemma 4.8).
2. Any irreducible polynomial in $\mathbb{Z}[x]$ is prime in $\mathbb{Z}[x]$ (Proposition 4.9). This is proved in two stages:
   (a) Let $p \in \mathbb{Z}$. If p is prime in $\mathbb{Z}$, then it is prime in $\mathbb{Z}[x]$ (Lemma 4.10).
   (b) Let f be an irreducible polynomial in $\mathbb{Z}[x]$ with $\deg(f) \geq 1$. Then f is prime in $\mathbb{Z}[x]$.

The proof in Chapter 12 also used Theorem 4.2, which we restate here for reference.

Theorem 1.12 *Theorem 4.2 of Chapter 12*

Let R be an integral domain in which every non-zero non-unit element has a factorisation into irreducible elements. Then R is a UFD if, and only if, every irreducible element in R is prime.

Our proof that a polynomial ring over a UFD is a UFD mimics that of Theorem 4.11. We state each of the above steps as a lemma.

Lemma 1.13

Let R be a UFD. Then every polynomial in $R[x]$ has a factorisation into irreducible polynomials in $R[x]$.

Proof Let $f(x) \in R[x]$ be a non-trivial element of $R[x]$. Then

$$f(x) = c_f f^*(x),$$

where $f^*(x)$ is a primitive polynomial. Since $c_f \in R$, either c_f is a unit, or it factorises uniquely (up to multiplication by a unit) in R as

$$c_f = p_1 p_2 \cdots p_s,$$

where each p_i is irreducible in R. Since p_i is irreducible in R, it is also irreducible in $R[x]$. We now have $f(x) = p_1 p_2 \cdots p_s f^*(x)$, so it suffices to show that every primitive polynomial in $R[x]$ has a factorisation into irreducibles. We will use a minimal counter-example argument. Let

$$S = \{f \in R[x] : f(x) \text{ is primitive, non-zero, not a unit and cannot be written as a product of irreducibles}\}.$$

We show that S is empty. Suppose for a contradiction that $f(x) \in S$. Then, by the Well-Ordering Principle (see Book A, Chapter 1, Subsection 3.2), we can pick f such that $\deg(f)$ is least among the degrees of polynomials in S.

Now, since f cannot be written as a product of irreducibles, it cannot itself be irreducible. Therefore we have a proper factorisation $f = ab$ for some polynomials $a, b \in R[x]$.

Note that we cannot have $\deg(a) = 0$, as then $a \in R$, and since f is primitive this would imply that a is a unit, so the factorisation $f = ab$ would not be proper. Thus $\deg(a) \geq 1$ and, symmetrically, $\deg(b) \geq 1$. Furthermore, by Lemma 1.10, both a and b must be primitive.

From $\deg(f) = \deg(ab) = \deg(a) + \deg(b)$ we have $\deg(a) < \deg(f)$ and $\deg(b) < \deg(f)$. Our choice of f implies that each of a and b is either irreducible or can be written as a product of irreducibles. This implies that $f = ab$ can be written as a product of irreducibles. This contradiction shows that S does not have an element of minimal degree, and therefore S must be empty, that is, all primitive polynomials can be written as a product of irreducibles. ■

Having established the existence of a factorisation into irreducibles for every element of $R[x]$, it remains to show that every irreducible element in $R[x]$ is prime in $R[x]$.

We start with a lemma that applies to polynomials of degree 0.

Lemma 1.14

Let R be an integral domain and let $R[x]$ be the ring of polynomials in one variable over R. If $p \in R$ is prime in R then it is prime in $R[x]$.

Proof We will use a minimal counter-example argument. Suppose that p is not prime in $R[x]$. Then there exist polynomials $f(x), g(x)$ with $\deg f = m$ and $\deg g = n$ such that p divides $f(x)g(x)$ but p divides neither $f(x)$ nor $g(x)$. Using the Well-Ordering Principle we can choose polynomials f and g so that $m + n$ is the least possible value for which this holds. Note that since p is prime in R, $m + n > 0$.

Now let $f(x) = a_m x^m + \cdots + a_0$ and
$g(x) = b_n x^n + \cdots + b_0$.
If p divides $f(x)g(x)$, then p must divide every coefficient in $f(x)g(x)$. Thus p divides the leading coefficient $a_m b_n$, and so, since p is prime in R, p divides either a_m or b_n. Without loss of generality, suppose that p divides a_m. Note that $m > 0$ since otherwise p divides $f(x)$. Then p divides

$$f(x)g(x) - a_m x^m g(x) = (f(x) - a_m x^m)g(x).$$

Now $f(x) - a_m x^m$ is of lower degree than $f(x)$. Since we chose $m + n$ to be minimal, and since p does not divide $g(x)$, we have that p divides $f(x) - a_m x^m$. However, this means that p divides

$$f(x) - a_m x^m + a_m x^m = f(x),$$

which contradicts our original assumption. Thus p must be prime in $R[x]$. ■

Lemma 1.15

Let R be a UFD, and f be an irreducible element in $R[x]$. Then f is prime in $R[x]$.

Proof Suppose f divides gh, where $g, h \in R[x]$. We need to show that f divides one of g or h. If $\deg(f) = 0$, then $f \in R$, and therefore f is prime in R by Theorem 4.2 of Book C, Chapter 12. Hence f is prime in $R[x]$ by Lemma 1.14.

Now suppose $\deg(f) > 0$. Then $f(x) = c_f g(x)$, where $g(x)$ is primitive. But f is irreducible, so c_f must be a unit and f itself is primitive in $R[x]$.

Let F denote the field of fractions of R. By Lemma 1.11, f is irreducible in $F[x]$, and since $F[x]$ is a Euclidean domain (see Book C, Chapter 12, Example 3.2(c)) f must be prime in $F[x]$ by Proposition 3.11 of Book C, Chapter 12. Thus since f divides gh in $F[x]$, either f divides g or f divides h, and without loss of generality we assume that f divides g.

Then there exists $s \in F[x]$ such that $fs = g$. We can write $s(x) = ct(x)$, where $c \in F$ and $t(x) \in R[x]$ is primitive. Therefore the following equation holds in $F[x]$:

$$f(x)(ct(x)) = g(x).$$

Since $c \in F$, we can write $c = \frac{a}{b}$ for some non-zero $a, b \in R$ with $\mathrm{hcf}(a, b) = 1$ (see Exercise 1.4). We want to show $c \in R$. Multiplying through by b gives

$$f(x)(at(x)) = bg(x).$$

We now consider the content of the polynomials on either side of this equation. On the left, the content is a, since f and t are primitive. On the right the content is bc_g, where c_g is the content of g, and this must be equal to the content on the left, so $a = bc_g$. However, $c_g \in R$, and so $c = \frac{a}{b} = c_g \in R$, and therefore $ct(x) \in R[x]$. Hence f divides g in $R[x]$, so f is prime in $R[x]$. ■

Theorem 1.16

Let R be a UFD. Then the polynomial ring $R[x]$ is a UFD.

Proof By Lemma 1.13, every non-zero, non-unit element of $R[x]$ has a factorisation into irreducibles. By Lemma 1.15, every irreducible element of $R[x]$ is prime. Therefore $R[x]$ is a UFD by Theorem 1.12. ■

We finish this section with an example of a ring, related to polynomial rings, that is also a UFD.

Example 1.17 *The ring of Laurent polynomials*

Let F be a field. Then

$$F[x, x^{-1}] = \{a_m x^m + \cdots + a_n x^n : a_i \in F \text{ for } i = m, \ldots, n \text{ with } m, n \in \mathbb{Z},\ m < n\}$$

is a ring, called the ring of **Laurent polynomials** over F. Note that since $m, n \in \mathbb{Z}$ the powers of x may be negative. For example,

$$5x^{-3} + 2x^{-1} + 5 + 7x^2$$

is a Laurent polynomial with $m = -3$ and $n = 2$.

$F[x, x^{-1}]$ is a subset of the field of fractions of $F[x]$, so to see that it is a ring we only need to observe that it is closed under both addition and multiplication, includes both the additive and multiplicative identities and includes additive inverses.

Laurent polynomials are named after the mathematician Pierre Alphonse Laurent (1813–1854). They are related to *Laurent series*, which are an important tool in complex analysis. A Laurent polynomial can be viewed as a Laurent series in which there are only finitely many non-zero coefficients.

We claim that $F[x, x^{-1}]$ is a Euclidean domain, and hence a UFD. To show that it is a Euclidean domain we need to show that it has a Euclidean norm (see Book C, Chapter 12, Definitions 2.14 and 3.1).

Let $f(x) = a_m x^m + \cdots + a_n x^n$ be in $F[x, x^{-1}]$ with a_m and a_n both non-zero, and define

$$N(f(x)) = n - m.$$

We claim that N is a Euclidean norm. Note that $N(x^v f(x)) = N(f(x))$ for all $v \in \mathbb{Z}$. The intuition is that the norm of a Laurent polynomial is, in some sense, a measure of its length, and multiplying the polynomial by a power of x just shifts it in one direction or the other without changing the length. Moreover, if $f(x) \in F[x]$, rather than $F[x, x^{-1}]$, and has a non-zero constant term, then $N(f(x)) = \deg f(x)$. More generally, if $f(x) \in F[x]$ then $N(f(x)) \leq \deg f(x)$.

To show N is a Euclidean norm, we need to show that, for $f, g \in F[x, x^{-1}]$,

(i) $N(f) \leq N(fg)$;

(ii) there exists $q, r \in F[x, x^{-1}]$ such that $f = gq + r$, and either $r = 0$ or $N(r) < N(g)$.

Let $f(x) = a_m x^m + \cdots + a_n x^n$ and
$g(x) = b_s x^s + \cdots + b_t x^t$
be two elements of $F[x, x^{-1}]$ with a_m, a_n, b_s, b_t all non-zero. Then $N(f) = n - m$, and since $a_n b_t \neq 0$ and $a_m b_s \neq 0$, we have that

$$N(fg) = (n + t) - (m + s) = (n - m) + (t - s) \geq N(f).$$

Thus condition (i) holds.

If $N(g) > N(f)$ then condition (ii) holds with $q = 0$ and $r = f$. We now show that condition (ii) also holds in the case $N(f) \geq N(g)$, that is $n - m \geq t - s$.

Consider $x^{-m} f = a_m + a_{m+1} x + \cdots + a_n x^{n-m}$ and
$x^{-s} g = b_s + b_{s+1} x + \cdots + b_t x^{t-s}$.
These are both polynomials in $F[x]$, which is a Euclidean domain. Therefore there are polynomials $q_1, r_1 \in F[x]$ such that

$$x^{-m} f = (x^{-s} g) q_1 + r_1,$$

where $r_1 = 0$ or $\deg(r_1) < \deg(x^{-s} g)$.

Then $f = x^{m-s} g q_1 + x^m r_1$. Let $q = x^{m-s} q_1$ and $r = x^m r_1$. Then:

- if $r_1 = 0$, then $r = 0$ and condition (ii) holds;
- otherwise, we know $\deg(r_1) < \deg(x^{-s} g)$, so $N(r_1) < N(x^{-s} g)$ in $F[x, x^{-1}]$. But $N(r_1) = N(r)$ and $N(x^{-s} g) = N(g)$ by what you observed after the definition of N. Therefore $N(r) < N(g)$, hence condition (ii) holds.

Since N is a Euclidean norm for $F[x, x^{-1}]$, $F[x, x^{-1}]$ is a Euclidean domain and hence a UFD.

2 Ideals

This section discusses ideals, which are special subsets of rings that play a similar role in ring theory as normal subgroups do in group theory. For example, the quotient of a ring by one of its ideals is again a ring, with suitably defined operations between the cosets of an ideal.

2.1 Ideals and their properties

In Book A, Chapter 3, Subsection 1.2 we described how the modular rings $\mathbb{Z}_n$ are constructed out of the ring $\mathbb{Z}$ by splitting $\mathbb{Z}$ up into the set of disjoint residue classes $\{[0], [1], \cdots, [n-1]\}$. For example, the elements of $\mathbb{Z}_3$ are the residue classes

$$[0] = \{\ldots, -6, -3, 0, 3, 6, \ldots\},$$
$$[1] = \{\ldots, -5, -2, 1, 4, 7, \ldots\},$$
$$[2] = \{\ldots, -4, -1, 2, 5, 8, \ldots\}.$$

Normally $\mathbb{Z}_3$ is represented by a complete set of residues modulo 3 such as $\{0, 1, 2\}$. We also showed that the operations of addition, subtraction and multiplication on residue classes are well defined by the rules

$$[a] \pm [b] = [a \pm b] \qquad \text{and} \qquad [a] \times [b] = [a \times b].$$

In this section we begin to explore whether this process can be generalised to rings other than $\mathbb{Z}$. Can we partition any ring R into subsets that form the elements of a new ring? If so, what does the zero element of such a ring look like? Two observations about the zero element $[0]$ of $\mathbb{Z}_n$ can guide us here. The first is that if we subtract $[0]$ from itself in $\mathbb{Z}_n$ then we must again obtain $[0]$. The second observation is that if we multiply $[0]$ by any element $[c] \in \mathbb{Z}_n$, we must also obtain $[0]$. These seemingly trivial observations tell us that the set $[0]$ must be closed under subtraction, and also under multiplication by elements of $\mathbb{Z}$. For if $c \in \mathbb{Z}$ and $a, b \in [0]$ then $[a] = [b] = [0]$, and so our two observations yield

$$[a - b] = [a] - [b] = [0] \qquad \text{and} \qquad [a \times c] = [a] \cdot [c] = [0].$$

Hence $a - b \in [0]$ and $a \cdot c \in [0]$, as suggested.

Subsets of a ring that have these two closure properties play a pivotal role in generalising the modular construction to arbitrary rings. They are called *ideals*.

Definition 2.1 *Ideal*

Let $(R, +, \cdot)$ be a commutative ring, and let I be a non-empty subset of R. Then I is an **ideal** of R if

I1 for all $a, b \in I$, $a - b \in I$

I2 for all $a \in I$ and $r \in R$, $ra \in I$.

Every ring R has at least two ideals, namely $\{0\}$ and R. It is sometimes convenient to be able to emphasise whether or not an ideal is one of these.

Definition 2.2 *Proper and non-trivial ideal*

An ideal I of a ring R is said to be **proper** if it is not equal to R. It is said to be **non-trivial** if it is not equal to $\{0\}$.

Any ideal I that contains the multiplicative identity 1 cannot be a proper ideal. This is because if $1 \in I$ and $a \in R$, then $a = a \cdot 1 \in I$ by I2. So $I = R$. It follows that a proper ideal of R cannot be a subring of R because it does not contain 1. Conversely, any ideal that does not contain 1 is proper.

By contrast, every ideal I contains the additive identity 0. Indeed, since I is non-empty it contains an element a, so $0 = a - a \in I$ by I1.

We emphasise these general properties of ideals below.

Let I be an ideal of the ring R. Then:

- $0 \in I$
- I is a proper ideal if, and only if, it does not contain the multiplicative identity 1.

Exercise 2.1

Let I be an ideal of a ring R and suppose that $a, b \in I$. Show that $a + b \in I$.

If we ignore the operation of multiplication on R for a moment, then we are left with a commutative group $(R, +)$, of which I is a normal subgroup by I1. In Section 3, we will show how the multiplication operation on R can be used to define a multiplication operation on the quotient group R/I, thereby turning it into a *quotient ring*. This will be the generalisation of the modular ring $\mathbb{Z}_n$ that we have been seeking. For now, however, we concentrate on exploring some further examples and properties of ideals.

Worked Exercise 2.3

Show that the set $I = \{f \in \mathbb{Z}[x] : f(3) = 0\}$ is an ideal of $\mathbb{Z}[x]$.

Solution

Since I contains the zero polynomial, it must be non-empty.

Moreover,

I1 if $f, g \in I$, then $(f-g)(3) = f(3) - g(3) = 0$, and so $f - g \in I$;

I2 if $f \in I$ and $r \in \mathbb{Z}[x]$, then $(rf)(3) = r(3)f(3) = r(3) \cdot 0 = 0$, so $rf \in I$.

So the ideal conditions are satisfied, and I is an ideal of $\mathbb{Z}[x]$.

Exercise 2.2

Let R be a commutative ring, and let $r \in R$. Show that the set

$$K = \{x \in R : xr = 0\}$$

is an ideal of R.

In the next exercise, we verify that the zero residue classes of a modular ring of integers, for example $[0] = \{\ldots, -6, -3, 0, 3, 6, \ldots\}$ in $\mathbb{Z}_3$, are ideals of $\mathbb{Z}$.

Worked Exercise 2.4

Let $n \in \mathbb{Z}$. Show that the set $n\mathbb{Z} = \{nk : k \in \mathbb{Z}\}$ is an ideal of $\mathbb{Z}$.

Solution

We first observe that $0 = n0 \in n\mathbb{Z}$, so $n\mathbb{Z}$ is non-empty.
Next we check the ideal conditions.

I1 Let nk_1 and nk_2 be two arbitrary elements of $n\mathbb{Z}$. Then

$$nk_1 - nk_2 = n(k_1 - k_2) \in n\mathbb{Z}.$$

I2 Let nk be an arbitrary element of $n\mathbb{Z}$ and let $m \in \mathbb{Z}$. Then

$$m(nk) = n(mk) \in n\mathbb{Z}.$$

We are using commutativity in $\mathbb{Z}$ here.

So $n\mathbb{Z}$ is an ideal of $\mathbb{Z}$.

Similarly, in the polynomial ring $\mathbb{Q}[x]$ the sets of all possible multiples of a given polynomial are ideals.

Exercise 2.3

Let q be a polynomial in $\mathbb{Q}[x]$. Show that the set

$$q\mathbb{Q}[x] = \{qk : k \in \mathbb{Q}[x]\}$$

is an ideal of $\mathbb{Q}[x]$.

In general, any set aR obtained by multiplying each element of a commutative ring R by a single element $a \in R$ is an ideal. Such a set is certainly non-empty, because $0 \in aR$, and moreover

I1 if $ar_1, ar_2 \in aR$, then $ar_1 - ar_2 = a(r_1 - r_2) \in aR$;

I2 if $k \in R$ and $ar \in aR$, then $k(ar) = a(kr) \in aR$.

So aR is indeed an ideal.

Such ideals occur sufficiently often to merit a special name.

Definition 2.5 *Principal ideal*

Let R be a commutative ring, and let $a \in R$. Then the set

$$aR = \{ar : r \in R\}$$

is the **principal ideal** of R generated by a. If the ring R is clear from the context, we often write $\langle a \rangle$ instead of aR.

Although in this book all the rings discussed are commutative, we have emphasised that R is commutative here as this is a definition.

Example 2.6 *Some principal ideals*

(a) In any ring R, the ideals generated respectively by 0 and 1 are

$$\langle 0 \rangle = 0\,R = \{0\} \quad \text{and} \quad \langle 1 \rangle = 1\,R = R.$$

(b) The ideal of $\mathbb{Z}$ generated by 5 is

$$\langle 5 \rangle = 5\mathbb{Z} = \{\ldots, -15, -10, -5, 0, 5, 10, 15, \ldots\}.$$

(c) The ideal of $\mathbb{Z}[i] = \{a + ib : a, b \in \mathbb{Z}\}$ generated by 5 is

$$\langle 5 \rangle = 5\mathbb{Z}[i] = \{5a + 5bi : a, b \in \mathbb{Z}\} = \{a + bi : a, b \in 5\mathbb{Z}\}.$$

(d) The ideal of $\mathbb{Z}[x]$ generated by x^2 is

$$\langle x^2 \rangle = x^2\mathbb{Z}[x] = \{a_0x^2 + a_1x^3 + \cdots + a_nx^{n+2} : a_0, a_1, \cdots, a_n \in \mathbb{Z}\}.$$

Exercise 2.4

Let R be a ring and let u be a unit in R. Show that $\langle u \rangle = R$.

The next exercise asks you to show that fields can be characterised among general rings in terms of their ideals.

Exercise 2.5

Show that a commutative ring F is a field if, and only if, it contains no proper non-trivial ideals.

In the next exercise, we use the notation $R[\alpha]$, where R is a subring of a ring S and α is an element of S, to denote the smallest subring of S that

contains R and α. For example, if α is a square root of an element in R, the set

$$\{a + b\alpha : a, b \in R\}$$

is a subring of S that contains both R and α, and you will see that

$$R[\alpha] = \{a + b\alpha : a, b \in R\}.$$

Exercise 2.6

Let R be a subring of S and suppose that $\alpha \in S$ with $\alpha^2 = r \in R$.

(a) Show that $T = \{a + b\alpha : a, b \in R\}$ is a subring of S.

(b) Show that $T = R[\alpha]$.

Exercise 2.7

Let $R = \mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} : a, b \in \mathbb{Z}\}$.

(a) Show that $\langle 1 + \sqrt{2} \rangle = R$.

(b) Write down a non-zero element x of R such that $\langle x \rangle \neq R$.

Now consider the following three principal ideals of $\mathbb{Z}$:

$$2\mathbb{Z} = \{\ldots, -8, -6, -4, -2, 0, 2, 4, 6, 8, \ldots\},$$
$$6\mathbb{Z} = \{\ldots, -24, -18, -12, -6, 0, 6, 12, 18, 24, \ldots\},$$
$$12\mathbb{Z} = \{\ldots, -48, -36, -24, -12, 0, 12, 24, 36, 48, \ldots\},$$

and notice that they satisfy $12\mathbb{Z} \subseteq 6\mathbb{Z} \subseteq 2\mathbb{Z}$. Notice, too, that $2 \mid 6$ and $6 \mid 12$. In the next exercise you are asked to show that this is an instance of a general property of the principal ideals of a ring.

Exercise 2.8

Let R be a ring, and let $a, b \in R$. Show that $aR \subseteq bR$ if, and only if, $b \mid a$.

The condition $b \mid a$ is equivalent to the condition $a \in bR$. Both are ways of saying that a is a multiple of b. We summarise these equivalences in the next lemma.

Lemma 2.7

Let R be a commutative ring, and let $a, b \in R$. Then the following statements are equivalent.

(a) $aR \subseteq bR$

(b) $b \mid a$

(c) $a \in bR$

Conditions (a) and (c) can also be written as $\langle a \rangle \subseteq \langle b \rangle$ and $a \in \langle b \rangle$ respectively.

Proof You showed that (a) ⇔(b) in the solution to Exercise 2.8. We are left to show that (b) ⇔ (c).

Suppose that $b \mid a$. Then there is an $s \in R$ such that $a = bs$, so $a \in bR$. Conversely, suppose that $a \in bR$. Then there is an element $s \in R$ such that $a = bs$ and so $b \mid a$. Thus we have shown (b) ⇔ (c) as required. ■

Exercise 2.9

We defined associates in Book C, Chapter 12, Definition 2.3.

Let R be an integral domain, and let $a, b \in R$. Show that $aR = bR$ if, and only if, a and b are associates.

A sequence of ideals such as

$$60\mathbb{Z} \subseteq 12\mathbb{Z} \subseteq 6\mathbb{Z} \subseteq 2\mathbb{Z},$$

in which each ideal is a subset of its successor, is known as a **chain of ideals**. A chain can consist of an infinite sequence of ideals,

$$I_0 \subseteq I_1 \subseteq I_2 \subseteq \cdots .$$

Infinite chains have a simple property that you are asked to explore in the next exercise.

Exercise 2.10

Let R be a ring, and let $I_0 \subseteq I_1 \subseteq I_2 \subseteq, \cdots$ be a chain of ideals of R.

Show that the union I of all the ideals I_n for $n = 0, 1, 2, \ldots$ is itself an ideal of R.

Do not be deceived by this exercise. There is no guarantee that an arbitrary union of ideals is an ideal. The solution to Exercise 2.10 depends crucially on the fact that the ideals form a chain. The next exercise shows this, and it also shows that intersections are better behaved.

Exercise 2.11

(a) Show that if I_1 and I_2 are ideals of a ring R then their intersection $I_1 \cap I_2$ is an ideal of R.

(b) By considering the ideals $I_1 = 2\mathbb{Z}$ and $I_2 = 7\mathbb{Z}$ of $\mathbb{Z}$, show that their union $I_1 \cup I_2$ is not an ideal of R.

Hint: for part (b), consider $2 - 7 = -5$ in $\mathbb{Z}$.

2.2 Principal ideal domains

Up to now, all of the ideals in $\mathbb{Z}$ that we have considered have been principal ideals consisting of all the multiples of some integer n. It seems natural to ask whether there are any ideals in $\mathbb{Z}$ that are not principal. The next theorem assures us that the answer is no.

Theorem 2.8

Every ideal in $\mathbb{Z}$ is a principal ideal. Every non-zero ideal in $\mathbb{Z}$ is generated by the smallest positive integer that it contains.

Proof Let I be an ideal in $\mathbb{Z}$. If $I = \langle 0 \rangle$, I is principal, so we can assume $I \neq \langle 0 \rangle$.

If $I \neq \langle 0 \rangle$, I must contain a positive integer, because it contains an integer m, and $m \in I \implies -m = (-1)m \in I$. Let n be the smallest positive integer in I.

First we show that n divides every element of I, so that $I \subseteq n\mathbb{Z}$. The proof uses the Euclidean Algorithm.

Let a be an arbitrary element of I and suppose that n does not divide a. Then, by the Euclidean Algorithm, there are integers k and r such that $a = kn + r$, where $0 < r < n$. Now, $a \in I$ and $n \in I$, and so $a - kn = r \in I$. But this contradicts the fact that n is the smallest positive integer in I, so it must be the case that n divides a and therefore $I \subseteq n\mathbb{Z}$.

For the reverse inclusion, since I is an ideal in $\mathbb{Z}$ and $n \in I$, it follows from closure under multiplication by elements of $\mathbb{Z}$ that $n\mathbb{Z} \subseteq I$. So $I = n\mathbb{Z}$, and we have shown that I is a principal ideal whose least positive element is a generator. ■

A very similar proof shows that every ideal I in the ring $\mathbb{Q}[x]$ is also principal, and it is generated by a polynomial of least degree in I. The underlying common feature here is that both $\mathbb{Z}$ and $\mathbb{Q}[x]$ are Euclidean domains, and so we can exploit the Euclidean Algorithm.

The following theorem is a generalisation of Theorem 2.8 to all Euclidean domains.

Theorem 2.9

Every ideal I in a Euclidean domain R is a principal ideal generated by an element with the least norm in I, or by 0 in the case $I = \{0\}$.

Proof Let R be a Euclidean domain with norm

$$d : R \setminus \{0\} \to \mathbb{N} \cup \{0\},$$

and let I be an ideal of R. If $I = \langle 0 \rangle$, I is principal, so we can assume $I \neq \langle 0 \rangle$. By the solution of Exercise 2.4, I is also principal if $1 \in I$, for then $I = \langle 1 \rangle = R$.

So let a be an element in I such that $a \neq 0$ and $0 < d(a) \leq d(b)$ for every $b \in I$. We show that a divides every element of I, and so $I \subseteq \langle a \rangle$ by Lemma 2.7.

Let b be an arbitrary element of I and suppose that a does not divide b. Then, by the Euclidean Algorithm, there are elements s and r in R such that $b = sa + r$, where $0 < d(r) < d(a)$.

Now $b \in I$ and $sa \in I$, and so $b - sa = r \in I$. But this contradicts the fact that a is an element in I with the least norm among all elements in I, and so it must be the case that a divides every element of I, and therefore $I \subseteq \langle a \rangle$.

For the reverse inclusion, since I is an ideal in R and $a \in I$, it follows from closure under multiplication that $\langle a \rangle \subseteq I$. So $I = \langle a \rangle$, and we have shown that I is a principal ideal whose generator is an element with least norm. ■

There is a special name for integral domains whose ideals are all principal.

Definition 2.10 *Principal ideal domain*

A **principal ideal domain** (PID) is an integral domain in which every ideal is principal.

The following corollary of Theorem 2.9 provides us with a rich supply of principal ideal domains.

Corollary 2.11

Every Euclidean domain is a principal ideal domain.

Corollary 2.11 tells us, for example, that the integers $\mathbb{Z}$, the Gaussian integers $\mathbb{Z}[i]$, and the ring of polynomials $F[x]$, where F is a field, are all examples of PIDs, for they are all Euclidean domains.

This raises the question as to whether there are any integral domains that have non-principal ideals. By Corollary 2.11, such a domain cannot be Euclidean, so it may be worth searching for an example in the integral domain $\mathbb{Z}[x]$, which was shown not to be Euclidean in Exercise 3.3(b) of Book C, Chapter 12.

Worked Exercise 2.12 *A non-principal ideal*

Let A be the set of polynomials in $\mathbb{Z}[x]$ that have an even constant term. Show that A is an ideal of $\mathbb{Z}[x]$ that is not principal.

Solution

First we observe that $0 \in A$, so A is non-empty. Next let

$$q(x) = 2a + a_1x + \cdots + a_nx^n \quad \text{and}$$
$$r(x) = 2b + b_1x + \cdots + b_mx^m$$

be two arbitrary elements of A, and

$$u(x) = c_0 + c_1x + \cdots + c_kx^k$$

be an arbitrary element of $\mathbb{Z}[x]$. Then

I1 the constant term of $q - r$ is $2(a - b)$, which is even, so $q - r \in A$;

I2 the constant term of uq is $2(c_0a)$, so $uq \in A$.

Thus A is an ideal of $\mathbb{Z}[x]$.

Now suppose that A is a principal ideal generated by a polynomial q. Since $2 \in A$, it follows that $2 = uq$ for some $u \in \mathbb{Z}[x]$. Then q must be a constant polynomial, otherwise
$\deg(uq) = \deg(u) + \deg(q) > 0 = \deg(2)$. But the polynomial x is an element of A, and so $x = vq$ for some $v \in \mathbb{Z}[x]$. Since q is constant, either $v = x$ and $q = 1$, or $v = -x$ and $q = -1$. Either way, q is an odd constant polynomial, which contradicts $q \in A$. So A is not principal.

It should be noted that the converse of Corollary 2.11 is not true: not all principal ideal domains are Euclidean domains. Nevertheless, some of the results that hold for Euclidean domains do carry over to PIDs. For example, highest common factors exist in PIDs.

For example, it can be shown that $\{\frac{1}{2}\left(a + b\sqrt{19}i\right) : a, b \in \mathbb{Z}\}$ is a subring of $\mathbb{C}$ that is a PID but not an ED. The proof, however, is rather technical, and beyond the scope of this module. It can be found in 'A Principal Ideal Domain That Is Not a Euclidean Domain', by Oscar A. Campoli, *The American Mathematical Monthly*, vol. 95, no. 9 (Nov. 1988), pp. 868–71.

Theorem 2.13 *Highest common factors in PIDs*

Let R be a principal ideal domain, and let $a, b \in R$. Then a and b have a highest common factor $\mathrm{hcf}(a, b)$, that is, a common factor that is a multiple of any other common factor.

Moreover, if $h = \mathrm{hcf}(a, b)$ then there are elements $s, t \in R$ such that $h = sa + tb$.

Proof Let $I = \{ua + vb : u, v \in R\}$. We leave you to check that I is an ideal of R. As R is a PID, there is an element $h \in R$ such that $I = \langle h \rangle$. Since $a \in I$ and $b \in I$, it follows that a and b are multiples of h, so $h \mid a$ and $h \mid b$. In other words, h is a common factor of a and b.

Since $h \in I$, there must be elements $s, t \in R$ such that $h = sa + tb$. So if $d \mid a$ and $d \mid b$ for some $d \in R$, then $d \mid (sa + tb)$, that is, $d \mid h$. So h is the highest common factor. Thus $h = \mathrm{hcf}(a, b)$ exists and $h = sa + tb$. ■

Had Worked Exercise 2.12 asked us to show that $\mathbb{Z}[x]$ is not a principal ideal domain, rather than check that A is not a principal ideal of $\mathbb{Z}[x]$, then we could have saved a little work simply by showing that there are no $s, t \in \mathbb{Z}[x]$ for which $\text{hcf}(2, x) = 1 = 2s(x) + xt(x)$, as we did in the solution to Exercise 3.3 of Book C, Chapter 12. The contrapositive form of Theorem 2.13 then confirms that $\mathbb{Z}[x]$ is not a principal ideal domain.

Worked Exercise 2.14

Find a highest common factor of the elements $3 + i$ and $1 + 3i$ in $\mathbb{Z}[i]$.

Solution

A highest common factor exists because $\mathbb{Z}[i]$ is a PID. In fact $\mathbb{Z}[i]$ is a Euclidean domain, so we can use the Euclidean Algorithm to find $\text{hcf}(3 + i, 1 + 3i)$. We begin by using ordinary complex division to obtain

$$\frac{3+i}{1+3i} = \frac{1}{10}(6 - 8i) = (1 - i) + \frac{1}{5}(-2 + i),$$

Multiply the numerator and the denominator by $1 - 3i$.

where $1 - i$ is the element of $\mathbb{Z}[i]$ closest to $\frac{1}{10}(6 - 8i)$. Then multiplying through by $1 + 3i$ gives the quotient–remainder form

$$3 + i = (1 - i)(1 + 3i) + (-1 - i).$$

An element of $\mathbb{Z}[i]$ is 'closest' to another in the sense of the Euclidean norm $N(a + bi) = a^2 + b^2$.

Since there is still a non-zero remainder, we calculate

$$\frac{1+3i}{-1-i} = -2 - i \in \mathbb{Z}[i].$$

The remainder is now zero, so an hcf is the previous remainder:

$$\text{hcf}(3 + i, 1 + 3i) = -1 - i.$$

Since -1 is a unit, $1 + i$ is also an hcf.

Exercise 2.12

Find a highest common factor, if one exists, of the elements $(9 + 11\sqrt{-2})$ and $(1 + 5\sqrt{-2})$ in $\mathbb{Z}[\sqrt{-2}]$.

We can use Theorem 2.13 to establish another result that carries over from Euclidean domains to PIDs.

Theorem 2.15

Let R be a principal ideal domain. Then p is prime in R if, and only if, p is an irreducible element of R.

Proof Since in any integral domain a prime is irreducible (see Book C, Chapter 12, Theorem 2.12), we are left to show that any irreducible element of R is prime.

Let $p \in R$ be irreducible, and suppose $p \mid ab$. Let $h = \text{hcf}(p, a)$ and write

$$h = up + va$$

for some $u, v \in R$.

If h is an associate of p, then $p \mid h$, and since $h \mid a$ it follows that $p \mid a$. If, on the other hand, h is not an associate of p, then the only way that h can divide p is if $p = rh$ for some non-unit $r \in R$. Since p is irreducible, this implies that h is a unit. We can therefore write

$$1 = h^{-1}(up + va),$$

and hence $b = (h^{-1}ub)p + (h^{-1}v)ab$. So b is divisible by p. In either case, p divides a or b, and so p is prime in R. ■

We can also show that every principal ideal domain is a unique factorisation domain (UFD).

Theorem 2.16 *Unique factorisation in PIDs*

Every principal ideal domain R is a unique factorisation domain.

Proof Let a_0 be any non-trivial element of R, where by 'non-trivial' we mean an element that is neither a unit nor zero. Suppose that a_0 cannot be expressed as a product of irreducible elements. Then a_0 cannot itself be irreducible, so $a_0 = a_1 b_1$ for some non-trivial $a_1, b_1 \in R$, at least one of which (a_1 say) cannot be expressed as a product of irreducibles. Then $a_1 = a_2 b_2$ for some non-trivial $a_2, b_2 \in R$, at least one of which (a_2 say) cannot be expressed as a product of irreducibles. Continuing in this way, we obtain a sequence

$$a_0, a_1, a_2, \ldots$$

where each element is a divisor of its predecessor. So by Lemma 2.7 we can form the chain

$$\langle a_0 \rangle \subseteq \langle a_1 \rangle \subseteq \langle a_2 \rangle \subseteq \cdots$$

of ideals in R. By the solution to Exercise 2.10, the union of all these ideals must itself be an ideal and it must therefore be equal to some principal ideal $\langle a \rangle$. Since a is an element of this union, it must also be an element of $\langle a_i \rangle$ for some i. So $\langle a \rangle \subseteq \langle a_i \rangle \subseteq \langle a_{i+1} \rangle \subseteq \langle a \rangle$ and we conclude that $\langle a_i \rangle = \langle a_{i+1} \rangle$. But this implies that a_i and a_{i+1} are associates by the solution to Exercise 2.9. Since this contradicts our previous statement that b_{i+1} is not a unit, we conclude that a_0 is in fact a product of irreducible elements.

The result now follows by Theorem 2.15 and Theorem 4.2 of Book C, Chapter 12. ■

We know from Theorem 4.5 and Corollary 4.6 of Book C, Chapter 12, that $\mathbb{Z}[x]$ is a UFD. However, you saw in Worked Exercise 2.12 that $\mathbb{Z}[x]$ is not a PID. We may therefore conclude that the converse of Theorem 2.16 is false: not all UFDs are PIDs.

Exercise 2.13

Decide whether or not each of the following rings is a PID, giving reasons for your answer.

(a) $\mathbb{Z}[\sqrt{-2}] = \{a + b\sqrt{-2} : a, b \in \mathbb{Z}\}$

(b) $\mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} : a, b \in \mathbb{Z}\}$

We close this section with a summary of the key results about various types of integral domain, and prime and irreducible elements. Figure 2.1 then shows the relationships between the various types of commutative rings we have discussed so far. It also gives examples that show that the inclusions are proper.

Results about different types of domain

- A polynomial ring in one variable over a field is a Euclidean domain (Book C, Chapter 11, Theorem 3.1).
- Every Euclidean domain is a principal ideal domain (Corollary 2.11).
- Every principal ideal domain is a unique factorisation domain (Theorem 2.16).
- If R is a unique factorisation domain then $R[x]$ is a unique factorisation domain (Theorem 1.16).
- Unique factorisation domains need not be Euclidean domains (Book C, Chapter 12, Example 4.5).
- Not all principal ideal domains are Euclidean domains (example cited in the margin note preceding Theorem 2.13).
- Not all unique factorisation domains are principal ideal domains. For example, $\mathbb{Z}[x]$ is a unique factorisation domain that is not a principal ideal domain.

Results about irreducible elements

- Let R be an integral domain and p a prime element in R. Then p is irreducible (Book C, Chapter 12, Theorem 2.12).
- Let R be a unique factorisation domain. Then p is prime in R if, and only if, p is an irreducible element of R (Book C, Chapter 12, Theorem 2.12 and Corollary 4.3).

- Let R be an integral domain in which every non-zero non-unit element has a factorisation into irreducible elements. Then R is a unique factorisation domain if, and only if, every irreducible element in R is prime (Book C, Chapter 12, Theorem 4.2).
- Let R be a unique factorisation domain and let $a, b \in R$. Then a and b have a highest common factor $\text{hcf}(a, b)$ (Book C, Chapter 12, Proposition 4.7).
- Let R be a principal ideal domain and let $a, b \in R$. Then a and b have a highest common factor $\text{hcf}(a, b)$. If $h = \text{hcf}(a, b)$, then there are elements $s, t \in R$ such that $h = sa + tb$ (Theorem 2.13).

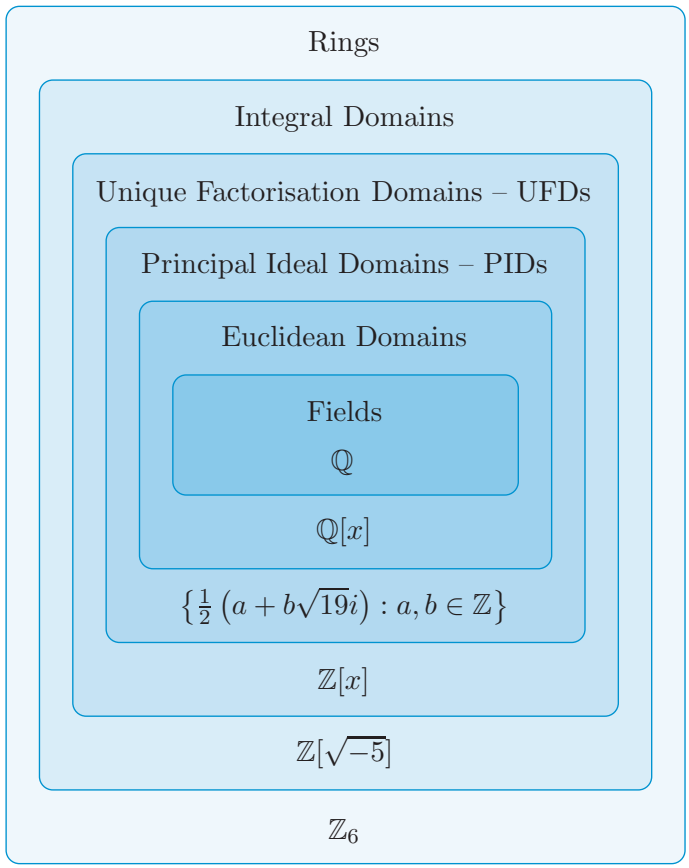


Figure 2.1 The relationships between different types of commutative rings

3 Operations on ideals

In Exercise 2.11(a) you saw that the intersection of two ideals is an ideal. This section explores other natural ways of obtaining new ideals from existing ones.

3.1 Sum of ideals

The next lemma will allow us to define an operation of addition between ideals.

Lemma 3.1

Let A and B be ideals of a ring R. Then the set

$$A + B = \{a + b : a \in A, b \in B\}$$

is an ideal of R.

Proof Since $0 + 0 = 0$, $A + B$ contains 0 and so it is non-empty. It remains to check conditions I1 and I2 of Definition 2.1.

I1 Let $a + b$ and $a_1 + b_1$ be arbitrary elements of $A + B$. Then

$$(a + b) - (a_1 + b_1) = (a - a_1) + (b - b_1) \in A + B.$$

I2 Let $a + b$ be an arbitrary element of $A + B$, and let $r \in R$. Then

$$r(a + b) = (ra) + (rb) \in A + B.$$

So $A + B$ is an ideal. ■

We can now define the sum of two ideals.

Definition 3.2 *Sum of two ideals*

The **sum of two ideals** A and B of a ring R is the ideal

$$A + B = \{a + b : a \in A, b \in B\}.$$

Exercise 3.1

Let A and B be ideals of a commutative ring R. Prove that

$$A \subseteq (A + B) \text{ and } B \subseteq (A + B).$$

Notice that since $A + B$ contains A and B, it must in fact be the smallest ideal containing A and B. To see this, let K be an ideal containing both A and B, and let $a + b \in A + B$ with $a \in A$ and $b \in B$. Then $a + b \in K$ by the solution to Exercise 2.1.

We now list some of the basic properties of addition of ideals.

Proposition 3.3 *Basic additive properties of ideals*

Let A, B and C be ideals of a commutative ring R. Then:

(a) $A \subseteq (A+B)$ and $B \subseteq (A+B)$

(b) $A+B = B+A$

(c) $(A+B)+C = A+(B+C)$

(d) $A+\{0\} = A$

(e) $A+R = R$.

Proof

(a) See the solution to Exercise 3.1.

(b) $A+B = \{a+b : a \in A, b \in B\}$
$= \{b+a : b \in B, a \in A\} = B+A$

(c) $(A+B)+C = \{u+c : u \in (A+B), c \in C\}$
$= \{(a+b)+c : a \in A, b \in B, c \in C\}$
$= \{a+(b+c) : a \in A, b \in B, c \in C\}$
$= \{a+v : a \in A, v \in (B+C)\}$
$= A+(B+C)$

(d) $A+\{0\} = \{a+0 : a \in A\} = A$

(e) By part (a), $R \subseteq A+R$, so $A+R = R$. ■

Exercise 3.2

In a principal ideal domain R, show that $\langle a \rangle + \langle b \rangle = \langle h \rangle$, where $h = \mathrm{hcf}(a,b)$.

3.2 Product of ideals

Next we consider how to define the product of two ideals I and J. By analogy with the definition of sum, the obvious candidate might appear to be the set of products $\{ab : a \in I, b \in J\}$. The snag is that this set is not usually closed under addition, and so it is not necessarily an ideal. The answer is to use arbitrary finite sums of products of an element of I and an element of J, that is, elements of the form

$$a_1b_1 + a_2b_2 + \cdots + a_nb_n,$$

in which any finite number n of terms is allowed.

Exercise 3.3

Let A and B be ideals in a ring R. Show that the set

$$AB = \{a_1b_1 + a_2b_2 + \cdots + a_nb_n : n \in \mathbb{N} \text{ and } a_i \in A, b_i \in B\},$$

is an ideal of R.

The solution to this exercise ensures that we can define the product of two ideals.

Definition 3.4 *Product of two ideals*

The **product of two ideals** A and B of a ring R is the ideal

$$AB = \{a_1b_1 + a_2b_2 + \cdots + a_nb_n : n \in \mathbb{N} \text{ and } a_i \in A, b_i \in B\}.$$

The sum and product share some of the same properties. They are, for example, both commutative and associative. However, there are also some differences. While the sum $A + B$ contains A and B, the product AB is contained in A and B. Also, the way in which the ideals $\{0\}$ and R combine with other ideals is very different.

Proposition 3.5 *Basic multiplicative properties of ideals*

Let A, B and C be ideals of a commutative ring R. Then:

(a) $AB \subseteq A$ and $AB \subseteq B$

(b) $AB = BA$

(c) $(AB)C = A(BC)$

(d) $A\{0\} = \{0\}$

(e) $AR = A$.

Proof In what follows we, adopt the convention that a, b, c (with or without subscripts) represent arbitrary elements of A, B, C, respectively.

(a) Let $x \in AB$. Then x is a sum of terms of the form ab, where $a \in A$ and $b \in B$. Each such ab belongs to both A and B, because ideals are closed under multiplication by elements of R, so x belongs to A and B.

That is, $AB \subseteq A$ and $AB \subseteq B$.

(b) Each element of AB has the form

$$a_1b_1 + \cdots + a_kb_k = b_1a_1 + \cdots + b_ka_k \in BA,$$

and each element of BA has the form

$$b_1a_1 + \cdots + b_ka_k = a_1b_1 + \cdots + a_kb_k \in AB.$$

So $AB = BA$.

(c) Let $x \in (AB)C$. Then x is a sum of elements of the form

$$(a_1b_1 + \cdots + a_kb_k)c = a_1(b_1c) + \cdots + a_k(b_kc),$$

so $x \in A(BC)$.

Now let $x \in A(BC)$. Then x is a sum of elements of the form

$$a(b_1c_1 + \cdots + b_\ell c_\ell) = (ab_1)c_1 + \cdots + (ab_\ell)c_\ell,$$

so $x \in (AB)C$. Hence $(AB)C = A(BC)$.

(d) By part (a), $A\{0\} \subseteq \{0\}$, so $A\{0\} = \{0\}$.

(e) Let $x \in A$. Then $x = x \cdot 1 \in AR$. So $A \subseteq AR$. But we also have $AR \subseteq A$ by part (a), hence $AR = A$. ■

3.3 Finitely generated ideals

Just as we defined the principal ideal generated by a single element, we now define the ideal generated by a finite subset $S = \{a_1, \ldots, a_n\}$ of a ring R. You met an ideal generated by two elements in the proof of Theorem 2.13, where you were left to check that

$$\{ua + vb : u, v \in R\}$$

is an ideal for two given elements a and b of a ring R. The next definition generalises this way to define an ideal.

Definition 3.6 *Ideal generated by a set*

Let R be a commutative ring. Then the **ideal of R generated by a finite subset** $S = \{a_1, \ldots, a_n\}$ of R is the set $\langle a_1, \ldots, a_n \rangle$ defined by

$$\langle a_1, \ldots, a_n \rangle = \{a_1r_1 + \cdots + a_nr_n : r_1, \ldots, r_n \in R\}.$$

The notation $\langle a_1, \ldots, a_n \rangle$ is sometimes abbreviated to $\langle S \rangle$.

The set $\langle a_1, \ldots, a_n \rangle$ is an ideal of R because it is the sum of n principal ideals:

$$\langle a_1, \ldots, a_n \rangle = a_1R + a_2R + \cdots + a_nR.$$

In fact, this sum is sometimes used to denote $\langle a_1, \ldots, a_n \rangle$ in cases where the ring under discussion needs to be highlighted.

Note that any given ideal may have many generating sets. In particular, although the ideal $\langle a_1, \ldots, a_n \rangle$ has more than one generator, it may or may not be principal. This fact is illustrated in the next exercise.

Exercise 3.4

Decide whether each of the following ideals is principal. If it is, find an element of the ring that generates it.

(a) The ideal $\langle 27, 36\rangle$ of the ring $\mathbb{Z}$.

(b) The ideal $\langle x, 2\rangle$ of the ring $\mathbb{Z}[x]$.

The approach used to find the generator of the ideal $\langle 27, 36\rangle$ in this exercise can be generalised to any PID.

Lemma 3.7

Let R be a PID, and let $a_1, a_2, \ldots, a_n \in R$. Then

$$\langle a_1, a_2, \ldots, a_n\rangle = \langle \mathrm{hcf}(a_1, a_2, \ldots, a_n)\rangle.$$

Proof The ideal $A = \langle a_1, a_2, \ldots, a_n\rangle$ is principal because R is a PID.

So let h be a generator of A. Then h is a common factor of every element of A, and in particular of the generators $a_1, a_2, \ldots, a_n$.

But $h \in A$, so $h = r_1a_1 + \cdots + r_na_n$ for some $r_1, r_2, \ldots, r_n \in R$. Therefore every common factor of $a_1, a_2, \ldots, a_n$ is also a factor of h.

In other words, $h = \mathrm{hcf}(a_1, a_2, \ldots, a_n)$. ■

Another approach to determining a generator for a principal ideal (or showing that one does not exist) is to use a multiplicative norm function to narrow down, or exclude, possible generators. For example, in $\mathbb{Z}[\sqrt{d}]$ we could take $N(a + b\sqrt{d}) = a^2 - db^2$ as such a norm. Then if an element of the ideal has norm 10, there is no point in looking for a generator that has norm 3, because $3 \nmid 10$.

Exercise 3.5

Decide whether or not each of the following ideals is principal. If it is, find an element of the ring that generates it.

(a) The ideal $A = \langle 3 + i, 1 + 3i\rangle$ of the ring $\mathbb{Z}[i]$.

(b) The ideal $A = \langle 2, 1 + \sqrt{-5}\rangle$ of the ring $\mathbb{Z}[\sqrt{-5}]$.

Hint: for part (b), use a multiplicative norm on $\mathbb{Z}[\sqrt{-5}]$.

The arguments in the solution to Exercise 3.5 are worth generalising. We do so in the next proposition.

Proposition 3.8

Let R be a commutative ring and suppose that $a_1, a_2, \ldots, a_n \in R$. Let A be an ideal of R. Then

$$\langle a_1, a_2, \ldots, a_n \rangle \subseteq A \text{ if, and only if, } a_1, a_2, \ldots, a_n \in A.$$

Proof Certainly $\langle a_1, a_2, \ldots, a_n \rangle \subseteq A$ implies that $a_1, a_2, \ldots, a_n \in A$.

Conversely, $a_1, a_2, \ldots, a_n \in A$ implies that $a_1R + a_2R + \cdots + a_nR \in A$, and so $\langle a_1, a_2, \ldots, a_n \rangle \subseteq A$. ■

Lemma 3.7 and Proposition 3.8 enable us to compare ideals by focusing on their generators. For example, Proposition 3.8 tells us that if we want to show that one ideal A is contained in another ideal B, then it is sufficient to show that the generators of A belong to B.

Exercise 3.6

(a) In the ring $\mathbb{Z}[x]$, show that $\langle x^2 - 1, x^2 - 2x + 1 \rangle$ is a subset of $\langle x - 1 \rangle$.

(b) In the ring $\mathbb{Z}[\sqrt{-5}]$, show that

(i) $\langle 2, 1 + \sqrt{-5} \rangle = \langle 2, 1 - \sqrt{-5} \rangle$

(ii) $\langle 9 \rangle \subseteq \langle 2 - \sqrt{-5} \rangle$.

The following result is useful, and it can be generalised to ideals with any finite number of generators.

Lemma 3.9

The product of the ideals $A = \langle a_1, a_2 \rangle$ and $B = \langle b_1, b_2 \rangle$ of a ring R is the ideal

$$I = \langle a_1b_1, a_1b_2, a_2b_1, a_2b_2 \rangle.$$

Proof The inclusion $I \subseteq AB$ follows from the definition of the product of two ideals and from Proposition 3.8.

The inclusion $AB \subseteq I$ follows from the fact that every element of the product AB is a sum of multiples of the elements $a_1b_1, a_1b_2, a_2b_1, a_2b_2$. ■

In particular, the product of an ideal of the form $\langle a, b \rangle$ with itself is the ideal $\langle a^2, ab, b^2 \rangle$. This is sometimes called the **square** of the ideal.

Worked Exercise 3.10

Let I be the ideal $\langle 2, 1+\sqrt{-5}\rangle$ in the ring $R = \mathbb{Z}[\sqrt{-5}]$. Show that

$$I^2 = 2R.$$

Solution

Since $(1+\sqrt{-5})^2 = -4+2\sqrt{-5}$, we have

$$I^2 = \langle 4, 2+2\sqrt{-5}, -4+2\sqrt{-5}\rangle.$$

Each of these three generators of I^2 can be shown to be in $2R$, hence $I^2 \subseteq 2R$ by Proposition 3.8.

Conversely, since $2R$ is generated by 2 and

$$2 = -4 + (2+2\sqrt{-5}) - (-4+2\sqrt{-5}),$$

we have that $2 \in I^2$, and so $2R \subseteq I^2$.

Therefore $I^2 = 2R$, as required.

Exercise 3.7

Let I be an ideal in a ring R and let $t \in R \setminus I$. Show that the set

$$\langle I, t\rangle = \{m + bt : b \in R, m \in I\}$$

is an ideal of R.

4 Quotients

Our initial reason for introducing ideals was to generalise the way in which the ring $\mathbb{Z}_n$ is constructed by partitioning the ring of integers $\mathbb{Z}$ into disjoint residue classes. We are now ready for this generalisation.

4.1 Cosets of an ideal

Any ring $(R, +, \cdot)$ can be regarded as an abelian group $(R, +)$ together with some extra axioms that govern the behaviour of the product. Each ideal I in R is a subgroup of $(R, +)$, because it is a non-empty set that is closed under subtraction (see Book B, Chapter 5, Proposition 2.5). Recall that any subgroup of an abelian group is normal. Therefore, an ideal of R is a normal subgroup of $(R, +)$. In Book B, Chapter 5, Subsection 2.2 you learnt that the cosets of a subgroup partition the host group into disjoint subsets. This is true in particular for any subgroup of $(R, +)$, but here we are interested only in those subgroups that are ideals, so we give the following definition.

Definition 4.1 *Cosets of an ideal*

Let I be an ideal of a ring R, and let $a \in R$. Then

$$a + I = \{a + r : r \in I\}$$

is the **coset** of I by a.

Note that we have used the coset notation for abelian groups here. This is appropriate since I is a subgroup of the abelian group $(R, +)$. This immediately gives us some useful results from group theory.

Proposition 4.2

Let R be a ring and I an ideal of R. Then the cosets of I partition R into disjoint subsets, and the following four statements are equivalent.

(a) $b - a \in I$

(b) $a + I = b + I$

(c) a and b are in the same coset of I

(d) $b \in a + I$

Proof The required results follow from Propositions 2.12 and 2.13 of Book B, Chapter 5. ■

We illustrate the equivalences in Proposition 4.2 in the following familiar example.

Example 4.3 *Cosets of an ideal in $\mathbb{Z}$*

The set $5\mathbb{Z}$ is an ideal in $\mathbb{Z}$, and its cosets partition $\mathbb{Z}$ into five disjoint subsets as follows.

$$\begin{aligned}
5\mathbb{Z} &= \{\ldots, -10, -5, 0, 5, 10, \ldots\} \\
1 + 5\mathbb{Z} &= \{\ldots, -9, -4, 1, 6, 11, \ldots\} \\
2 + 5\mathbb{Z} &= \{\ldots, -8, -3, 2, 7, 12, \ldots\} \\
3 + 5\mathbb{Z} &= \{\ldots, -7, -2, 3, 8, 13, \ldots\} \\
4 + 5\mathbb{Z} &= \{\ldots, -6, -1, 4, 9, 14, \ldots\}
\end{aligned}$$

We can see from this list that 2 and 3 are in different cosets, and that

$$\begin{aligned}
3 - 2 = 1 &\notin 5\mathbb{Z}, \\
2 + 5\mathbb{Z} &\neq 3 + 5\mathbb{Z}, \\
2 &\notin 3 + 5\mathbb{Z}.
\end{aligned}$$

On the other hand, 3 and -7 are in the same coset, and

$$\begin{aligned}
3 - (-7) = 10 &\in 5\mathbb{Z}, \\
3 + 5\mathbb{Z} &= -7 + 5\mathbb{Z}, \\
-7 &\in 3 + 5\mathbb{Z}.
\end{aligned}$$

Our discussion so far has depended solely on the additive structure of the ring R. However, our aim is not to construct a quotient group from the set of the cosets as we did in the group theory chapters, but rather to construct a quotient *ring*.

While a quotient group requires a single operation to be defined on the set of cosets, a quotient ring requires two, namely addition and multiplication. We already know how to define addition from group theory: if $a+I$ and $b+I$ are two arbitrary cosets of I by a and b respectively, then

$$(a+I)+(b+I)=(a+b)+I.$$

The definition of multiplication is as expected:

$$(a+I)(b+I)=(ab)+I.$$

Before continuing, we must check that this operation of multiplication is well defined. So suppose that $a+I=c+I$ and $b+I=d+I$. Then by Proposition 4.2 we have $a-c\in I$ and $b-d\in I$, so

$$ab-cd=(a-c)b+c(b-d)\in I,$$

using the fact that I is closed under multiplication by any ring elements (here c and b). It follows that $ab+I=cd+I$, and so multiplication is well defined.

We are now close to our goal of defining a quotient ring. You are asked to do some preliminary work in the next exercise.

Exercise 4.1

Let R be a ring, and I be an ideal of R. Show that the set of cosets

$$S=\{a+I : a\in R\}$$

forms a ring under the operations of coset addition $+$ and coset multiplication $\cdot$ defined above.

Our conclusions about the ring $(S,+,\cdot)$ are summarised in the next theorem.

Theorem 4.4

Let I be an ideal of a ring R. Then the set of cosets of I in R, with the operations $+$ and $\cdot$ defined by

$$(a+I)+(b+I)=(a+b)+I \quad \text{and}$$
$$(a+I)\cdot(b+I)=ab+I$$

is a ring, called the **quotient ring** of R by I, and denoted by R/I.

The additive identity of R/I is $0+I$, the multiplicative identity is $1+I$, and the additive inverse of $a+I$ is $-a+I$.

In deriving the above result we have made extensive use of the fact that an ideal of a ring R is also a subgroup of the additive group $(R, +)$. It is very important to realise that the converse is not true: an additive subgroup of R is not necessarily an ideal of R, as the following example illustrates.

Example 4.5 *A subgroup that is not an ideal*

Let $R = \mathbb{Z}[i]$ be the ring of Gaussian integers. Then $\mathbb{Z}$ is a subgroup of $(R, +)$, but $\mathbb{Z}$ is not an ideal of R. This is because any ideal of R that contains the identity element 1 is equal to R, so $\mathbb{Z}$ cannot be an ideal of $\mathbb{Z}[i]$.

We illustrate the process of forming the quotient of a ring through the example of a quotient of the polynomial ring $\mathbb{Q}[x]$.

Worked Exercise 4.6

Let $R = \mathbb{Q}[x]$, and let I be the ideal $\langle x^2 + 1 \rangle$ of R.

(a) Describe the set of cosets R/I.

(b) Find formulas for the coset operations of addition and multiplication.

Solution

(a) Each coset of I has the form $f(x) + I$, where $f \in \mathbb{Q}[x]$. By the Division Algorithm we can write

$$f(x) = q(x)(x^2 + 1) + r(x),$$

where $q, r \in \mathbb{Q}[x]$ and $\deg(r) < \deg(x^2 + 1) = 2$. So

$$f(x) - r(x) = q(x)(x^2 + 1) \in I.$$

Then, by Proposition 4.2,

$$f(x) + I = r(x) + I.$$

But $\deg(r) < 2$, so $r(x)$ has the form $a + bx$, and

$$R/I = \{(a + bx) + I : a, b \in \mathbb{Q}\}.$$

Moreover, $(a + bx) + I = (c + dx) + I$ gives

$$(a + bx) - (c + dx) = (a - c) + (b - d)x \in I,$$

and this is only possible if $a = c$ and $b = d$.

(b) If $a + bx + I$ and $c + dx + I$ are arbitrary elements of R/I, then

$$\begin{aligned}(a + bx + I) + (c + dx + I) &= (a + bx) + (c + dx) + I \\ &= (a + c) + (b + d)x + I.\end{aligned}$$

The product introduces a term in x^2 that we can absorb into I:

$$\begin{aligned}(a+bx+I)\cdot(c+dx+I) &= (a+bx)(c+dx)+I\\ &= ac+(ad+bc)x+bdx^2+I\\ &= (ac-bd)+(ad+bc)x\\ &\quad +bd(x^2+1)+I\\ &= (ac-bd)+(ad+bc)x+I.\end{aligned}$$

Alternatively, we could have gone directly from the second line to the fourth by replacing x^2 by -1. This works because $x^2+1\in I$, and so x^2+1, or rather x^2+1+I, is the additive identity in the quotient ring R/I.

It may have struck you that the formulas for multiplying and adding the cosets in Worked Exercise 4.6 resemble the formulas for adding and multiplying complex numbers. Indeed, if we ignore every '$+I$' and replace every x by i, we end up with valid formulas for adding and multiplying the elements of $\mathbb{Q}[i]$, namely

$$(a+bi)+(c+di)=(a+c)+(b+d)i \quad \text{and}$$
$$(a+bi)\cdot(c+di)=(ac-bd)+(ad+bc)i.$$

In this sense, we can say that $\mathbb{Q}[x]/I$ and $\mathbb{Q}[i]$ look like the same ring. There is a rigorous way to express this resemblance mathematically, and we will discuss this in Subsection 4.3. In the meantime, here is a similar quotient for you to work out.

Exercise 4.2

Let $R=\mathbb{Q}[x]$, and let I be the ideal $\langle x^2+x+1\rangle$ of R.

(a) Describe the set of cosets R/I.

(b) Find formulas for the coset operations of addition and multiplication.

In the solution to Exercise 4.2, the underlying set of the quotient ring $\mathbb{Q}[x]/I$ is $\{(a+bx)+I : a,b\in\mathbb{Q}\}$. This underlying set resembles that of many other rings in this module, for example $\mathbb{Q}[i], \mathbb{Q}[\sqrt{-2}]$ and $\mathbb{Q}[\sqrt{-5}]$. However, none of these rings has a similar multiplicative operation to the one we have found, so any further description of a similarity with a quotient of $\mathbb{Q}[x]$ is not straightforward. We will look at quotients of this kind in much more detail in Chapter 18.

4.2 Homomorphisms

In the paragraph following Worked Exercise 4.6, we remarked that the quotient ring $\mathbb{Q}[x]/\langle x^2+1\rangle$ looks like the ring $\mathbb{Q}[i]$. By contrast, the solution to Exercise 4.2 suggested that the quotient ring $\mathbb{Q}[x]/\langle x^2+x+1\rangle$ is harder to identify. To help us make more systematic comparisons between rings, we introduce ring homomorphisms, which are functions that preserve the ring operations.

Definition 4.7 *Ring homomorphism*

Let R and S be rings. A **ring homomorphism** is a function $f\colon R \to S$ such that, for all $a, b \in R$:

$$f(a+b) = f(a) + f(b)$$
$$f(ab) = f(a)f(b)$$
$$f(1_R) = 1_S,$$

where 1_R and 1_S are the multiplicative identities in R and S respectively.

When S is an integral domain, the condition $f(1_R) = 1_S$ follows from the first two, and may be omitted.

When the fact that f is a function between rings is clear from the context, we often say that f is a homomorphism, rather than a ring homomorphism. We often refer to the two properties in Definition 4.7 as the *homomorphism* or *morphism properties* for addition and multiplication, respectively. This is consistent with the terminology introduced after Definition 1.4.

A ring homomorphism may or may not be one–one, and it may or may not be onto. The following examples illustrate some of the possibilities.

Example 4.8 *Some ring homomorphisms*

(a) Let R be a ring, and let $f\colon R \to R$ be the identity function $f(x) = x$. Then f is a ring homomorphism that is both one–one and onto.

(b) The function $f\colon \mathbb{Z} \to \mathbb{Q}$ defined by $f(x) = x$ is a homomorphism that is one–one but not onto.

(c) The function $f\colon \mathbb{Z} \to \mathbb{Z}_n$ defined by $f(x) = x \pmod n$ is a ring homomorphism that is onto but not one–one.

(d) Let $f\colon \mathbb{C} \to \mathbb{C}$ be the conjugation function $f(a+ib) = a - ib$. Then f is a homomorphism that is one–one and onto.

Exercise 4.3

Show that each of the following functions is a homomorphism.

(a) The function $f\colon \mathbb{Z}[x] \to \mathbb{Z}_2$ defined by $f(r) = r(0) \pmod 2$.

(b) The function $f\colon \mathbb{Q}[\sqrt{5}] \to \mathbb{Q}[\sqrt{5}]$ defined by $f(a+b\sqrt{5}) = a - b\sqrt{5}$.

(c) The function $f\colon \mathbb{Z} \to \mathbb{C}$ defined by $f(x) = x + 0i$.

Since a homomorphism preserves the behaviour of the ring operation, it is not unreasonable to expect some of the ring properties to be preserved too. This is indeed the case.

Proposition 4.9 *Basic properties of homomorphisms*

Let $f: R \to S$ be a ring homomorphism. Then:

(a) $f(0_R) = 0_S$, where 0_R and 0_S are the additive identities of R and S respectively

(b) $f(-a) = -f(a)$ for all $a \in R$

(c) if u is a unit in R, then $f(u)$ is a unit in S.

The proof of Proposition 4.9 is left as an exercise.

Exercise 4.4

Prove Proposition 4.9.

In Example 4.8 we saw two ring homomorphisms that were both one–one and onto. Homomorphisms with these properties are known as isomorphisms, and we already defined them in Definition 1.4. An isomorphism between a ring and itself, such as complex conjugation in Example 4.8(d), has a special name.

Definition 4.10 *Ring automorphism*

A ring isomorphism $f: R \to R$ whose domain and codomain are the same ring R is known as a ring **automorphism**.

As in group theory and linear algebra, there are two special sets associated with a ring homomorphism.

Definition 4.11 *Image and kernel*

Let R and S be rings, and $f: R \to S$ a ring homomorphism.

(a) The **image** of f is the set $\mathrm{Im}(f) = \{f(a) : a \in R\}$.

(b) The **kernel** of f is the set $\mathrm{Ker}(f) = \{a \in R : f(a) = 0\}$.

As in the case of group homomorphisms, the image of a ring homomorphism is a subset of the codomain and the kernel is a subset of the domain, so if $f: R \to S$ is a ring homomorphism then

$$\mathrm{Im}(f) \subseteq S \quad \text{and} \quad \mathrm{Ker}(f) \subseteq R.$$

The kernel and image can be used to check whether or not a given homomorphism is one–one or onto.

Proposition 4.12

Let $f: R \to S$ be a ring homomorphism. Then:

(a) f is onto if, and only if, $\mathrm{Im}(f) = S$

(b) f is one–one if, and only if, $\mathrm{Ker}(f) = \{0\}$.

Proof

(a) If $S = \mathrm{Im}(f)$, then any element of S can be written as $f(r)$ for some $r \in R$, so f is onto.

Conversely, if f is onto then for any $s \in S$ there is $r \in R$ such that $s = f(r)$, so $s \in \mathrm{Im}(f)$. Therefore $S = \mathrm{Im}(f)$.

(b) Suppose f is one–one. If $a \in \mathrm{Ker}(f)$, then $f(a) = 0$, so $f(0) = 0 = f(a)$. But f is one–one, so $a = 0$ and hence $\mathrm{Ker}(f) = \{0\}$.

Conversely, suppose that $\mathrm{Ker}(f) = \{0\}$. If $f(a) = f(b)$, then $f(a - b) = f(a) - f(b) = 0$. Thus $a - b \in \mathrm{Ker}(f) = \{0\}$, and hence $a - b = 0$, so $a = b$. It follows that f is one–one. ■

Example 4.13 *Kernel and image of a homomorphism*

Consider the homomorphism $f: \mathbb{Z}[x] \to \mathbb{Z}$ defined by $f(r) = r(0)$. That is, f maps each polynomial in $\mathbb{Z}[x]$ to its constant coefficient.

We have that $\mathrm{Im}(f)$ is the whole of $\mathbb{Z}$, for if $a \in \mathbb{Z}$ then $f(a + x) = a$, and so $\mathrm{Im}(f) = \mathbb{Z}$.

To find $\mathrm{Ker}(f)$, let $r \in \mathbb{Z}[x]$ with $f(r) = 0$, so $r(0) = 0$. Then

$$\mathrm{Ker}(f) = \{r : r \text{ has constant coefficient } 0\},$$

and $\mathrm{Ker}(f) \neq \{0\}$. It follows that f is onto but not one–one.

Exercise 4.5

Find the image and kernel of each of the following homomorphisms from Exercise 4.3. Decide whether the homomorphism is onto and/or one–one.

(a) $f: \mathbb{Z}[x] \to \mathbb{Z}_2$ defined by $f(r) = r(0) \pmod 2$.

(b) $f: \mathbb{Z}[\sqrt{5}] \to \mathbb{Z}[\sqrt{5}]$ defined by $f(a + b\sqrt{5}) = a - b\sqrt{5}$.

(c) $f: \mathbb{Z} \to \mathbb{C}$ defined by $f(x) = x + 0i$.

You may have noticed that the kernel of f in the solution to Exercise 4.5(a) is the ideal of $\mathbb{Z}[x]$ that we discussed in Worked Exercise 2.12. Again, in each of parts (b) and (c), the kernel of f is the trivial ideal, that is, $\{0\}$. It turns out that the kernel of a homomorphism is always an ideal, and the image is always a subring.

Proposition 4.14

Let R and S be rings, and $f: R \to S$ a ring homomorphism. Then:

(a) $\mathrm{Im}(f)$ is a subring of S

(b) $\mathrm{Ker}(f)$ is an ideal of R.

Proof

(a) Since $0 = f(0)$, $\mathrm{Im}(f)$ contains 0, and so it is non-empty. We check the subring criteria (Book C, Chapter 11, Lemma 1.8). Let $a, b \in \mathrm{Im}(f)$. Then $a = f(c)$ and $b = f(d)$ for some $c, d \in R$, so

SR1 $a - b = f(c) - f(d) = f(c - d) \in \mathrm{Im}(f)$

SR2 $ab = f(c)f(d) = f(cd) \in \mathrm{Im}(f)$

SR3 $f(1) = 1$, so $\mathrm{Im}(f)$ contains the multiplicative identity 1.

It follows that $\mathrm{Im}(f)$ is a subring of S.

(b) Since $\mathrm{Ker}(f)$ contains zero, the additive identity, it must be non-empty. Moreover,

I1 if $a, b \in \mathrm{Ker}(f)$, then $f(a) = f(b) = 0$ and so $f(a - b) = f(a) - f(b) = 0$, giving $a - b \in \mathrm{Ker}(f)$;

I2 if $a \in \mathrm{Ker}(f)$ and $r \in R$, then $f(a) = 0$ and so $f(ra) = f(r)f(a) = 0$, so $ra \in I$.

So the ideal conditions are satisfied, and $\mathrm{Ker}(f)$ is an ideal of R. ■

We can say more, as the following proposition shows.

Proposition 4.15

Let I be an ideal of a ring R. Then there is a homomorphism $f: R \to R/I$ such that $\mathrm{Ker}(f) = I$.

Proof Let f be defined by

$$f(a) = a + I.$$

Then $f(1) = 1 + I$, and for all $a, b \in R$

$$f(a + b) = (a + b) + I = (a + I) + (b + I) = f(a) + f(b), \quad \text{and}$$

$$f(ab) = ab + I = (a + I)(b + I) = f(a)f(b).$$

So f is a homomorphism.

By Proposition 4.2, $f(a) = a + I$ is equal to the additive identity I of R/I if, and only if, $a \in I$. So $\mathrm{Ker}(f) = I$. ■

The function defined in the above proposition is known as the *natural homomorphism* from R to R/I.

Definition 4.16 *Natural homomorphism*

Let I be an ideal of a ring R. Then the **natural homomorphism** from R to R/I is the function

$$\begin{aligned} f \;:\; & R \to R/I \\ & a \mapsto a + I. \end{aligned}$$

Another homomorphism that we will find useful is the modulo function

$$\hat{f}_p : \mathbb{Z}[x] \to \mathbb{Z}_p[x]$$

that takes each polynomial with integer coefficients, and reduces its coefficients modulo some prime number p, that is,

$$\hat{f}_p(a_0 + a_1 x + \cdots + a_n x^n) = \hat{a}_0 + \hat{a}_1 x + \cdots + \hat{a}_n x^n,$$

where $a_i \equiv \hat{a}_i \pmod{p}$, for $i = 1, 2, \ldots, n$. Some texts refer to this as the **canonical homomorphism**. In Book C, Chapter 11, Lemma 4.19, we showed that a polynomial with leading coefficient not divisible by p is irreducible if it is irreducible in $\mathbb{Z}_p$. The proof of the lemma uses the homomorphism $\hat{f}_p$ in an essential way.

Exercise 4.6

Find the kernel of the modulo function $\hat{f}_p$ defined above.

4.3 The First Isomorphism Theorem

If we are given a one–one ring homomorphism $f\colon R \to S$, we cannot in general say that R is isomorphic to S, because f may not be onto. We can, however, say that R is isomorphic to $\mathrm{Im}(f)$. Indeed, we could simply redefine the codomain of f to be $\mathrm{Im}(f)$, thereby turning f into an isomorphism.

But what happens if f is not one–one? We will show that $\mathrm{Im}(f)$ is then isomorphic to the quotient $R/\operatorname{Ker}(f)$. The quotient is a ring because $\operatorname{Ker}(f)$ is an ideal of R by Proposition 4.14(b).

Theorem 4.17 *First Isomorphism Theorem*

Let $f\colon R \to S$ be a ring homomorphism from a ring R to a ring S. Then the function $\psi : R/\operatorname{Ker}(f) \to \mathrm{Im}(f)$ defined by

$$\psi : a + \operatorname{Ker}(f) \mapsto f(a)$$

is an isomorphism.

Proof Firstly, since ψ is defined in terms of a representative a of the coset $a + \operatorname{Ker}(f)$ rather than in terms of $a + \operatorname{Ker}(f)$ itself, we must check that ψ is well defined.

For this, we need to show that if a and $b \in R$ are such that $a + \mathrm{Ker}(f) = b + \mathrm{Ker}(f)$, then $\psi(a + \mathrm{Ker}(f)) = \psi(b + \mathrm{Ker}(f))$. But if $a + \mathrm{Ker}(f) = b + \mathrm{Ker}(f)$ then $(b - a) \in \mathrm{Ker}(f)$ by Proposition 4.2, and so $0 = f(b - a) = f(b) - f(a)$. Hence $f(a) = f(b)$, that is $\psi(a + \mathrm{Ker}(f)) = \psi(b + \mathrm{Ker}(f))$, as required.

Secondly, we check that ψ is a bijection. For this, suppose $\psi(a + \mathrm{Ker}(f)) = 0$. Then $f(a) = 0$, and hence $a \in \mathrm{Ker}(f)$. So $a + \mathrm{Ker}(f) = \mathrm{Ker}(f)$ is the additive identity of $R/\mathrm{Ker}(f)$, and so ψ is one–one by Proposition 4.12(b).

To see that ψ is onto, it suffices to note that an element $f(a) \in \mathrm{Im}(f)$ is the image of $a + \mathrm{Ker}(f) \in R/\mathrm{Ker}(f)$ under ψ.

Finally, we check that ψ satisfies the conditions in Definition 1.4. Let $a + \mathrm{Ker}(f)$ and $b + \mathrm{Ker}(f)$ be arbitrary elements of $R/\mathrm{Ker}(f)$. Then

- $$\begin{aligned}\psi\left((a + \mathrm{Ker}(f)) + (b + \mathrm{Ker}(f))\right) &= \psi\left((a + b) + \mathrm{Ker}(f)\right)\\ &= f(a + b)\\ &= f(a) + f(b)\\ &= \psi\left(a + \mathrm{Ker}(f)\right) + \psi(b + \mathrm{Ker}(f))\end{aligned}$$
- $$\begin{aligned}\psi\left((a + \mathrm{Ker}(f)) \cdot (b + \mathrm{Ker}(f))\right) &= \psi\left(ab + \mathrm{Ker}(f)\right)\\ &= f(ab)\\ &= f(a)f(b)\\ &= \psi\left(a + \mathrm{Ker}(f)\right)\psi\left(b + \mathrm{Ker}(f)\right).\end{aligned}$$

Moreover,

- $\psi(1 + \mathrm{Ker}(f)) = f(1) = 1$, so ψ maps the multiplicative identity of $R/\mathrm{Ker}(f)$ to the multiplicative identity of $\mathrm{Im}(f)$.

Thus, ψ is an isomorphism between $R/\mathrm{Ker}(f)$ and $\mathrm{Im}(f)$, as required. ■

Example 4.18 *The modular ring $\mathbb{Z}_5$*

The isomorphism $\mathbb{Z}/5\mathbb{Z} \cong \mathbb{Z}_5$ can be written in the form

$$\mathbb{Z}/\mathrm{Ker}(f) \cong \mathrm{Im}(f),$$

where $f : \mathbb{Z} \to \mathbb{Z}_5$ is the function defined by

$$f(x) = x \pmod 5.$$

This is because $f(x) = 0 \in \mathbb{Z}_5$ if, and only if, $x \equiv 0 \pmod 5$, that is, x is a multiple of 5, so $\mathrm{Ker}(f) = 5\mathbb{Z}$. Moreover, $\mathrm{Im}(f) = \mathbb{Z}_5$ because of the way that f has been defined.

Hence this isomorphism can be obtained by Theorem 4.17.

In Worked Exercise 4.6 we made the observation that if $I = \langle x^2 + 1\rangle$, then the quotient ring $\mathbb{Q}[x]/I$ looks like the ring $\mathbb{Q}[i]$. In support of this we noted that the ring operations for adding and multiplying cosets are

$$(a + bx + I) + (c + dx + I) = (a + c) + (b + d)x + I,$$
$$(a + bx + I) \cdot (c + dx + I) = (ac - bd) + (ad + bc)x + I.$$

If we ignore every '$+I$' and replace every x by i, we obtain the formulas for adding and multiplying the elements of $\mathbb{Q}[i]$, namely

$$(a+bi)+(c+di)=(a+c)+(b+d)i,$$
$$(a+bi)\cdot(c+di)=(ac-bd)+(ad+bc)i.$$

This suggests that $\mathbb{Q}[x]/I$ is isomorphic to $\mathbb{Q}[i]$. This is indeed the case, and in the next subsection we will use the First Isomorphism Theorem to make these ideas more precise, not just for the ring $\mathbb{Q}[i]$, but also for rings like $\mathbb{Q}[\sqrt{2}]$, $\mathbb{Q}[\sqrt{-3}]$ and $\mathbb{Q}[\sqrt{-5}]$. In Chapter 18 we will see that these are all, in fact, fields.

4.4 Quotient rings of $K[x]$

In this subsection, we will look at quotient rings of $K[x]$, where K is a field and the ideal by which we quotient is generated by an irreducible polynomial. We start with the special case $K=\mathbb{Q}$.

So suppose that $p(x)$ be an irreducible polynomial in $\mathbb{Q}[x]$, and consider the ideal $P=\langle p(x)\rangle$.

In order to relate quotient rings such as $\mathbb{Q}[x]/P$ to rings such as $\mathbb{Q}[i]$, we would like to find a homomorphism from $\mathbb{Q}[x]$ to $\mathbb{C}$, the field of complex numbers, whose kernel is P. This would allow us to use the First Isomorphism Theorem to describe $\mathbb{Q}[x]/P$ as a subring of $\mathbb{C}$.

For a start, we know that the kernel of such a homomorphism is P if any multiple of the irreducible polynomial $p(x)$ is mapped to zero. It will help to introduce certain maps from $\mathbb{Q}[x]$ to $\mathbb{C}$.

Definition 4.19 *Evaluation homomorphism*

Let $\alpha\in\mathbb{C}$. Then the function $f_\alpha:\mathbb{Q}[x]\to\mathbb{C}$ defined by

$$f_\alpha(a_0+a_1x+\cdots+a_nx^n)=a_0+a_1\alpha+\cdots+a_n\alpha^n$$

is called an **evaluation homomorphism**.

The functions f_α defined in this way are indeed homomorphisms, and before we proceed we need to check this. In the next exercise you are asked to show that an evaluation homomorphism satisfies the first condition in Definition 4.7.

Exercise 4.7

Let $\alpha\in\mathbb{C}$, and let f_α be the evaluation homomorphism in Definition 4.19. Show that for p and $q\in\mathbb{Q}[x]$

$$f_\alpha(p+q)=f_\alpha(p)+f_\alpha(q).$$

We now need to check that an evaluation homomorphism f_α satisfies the second condition in Definition 4.7, that is, for p and $q \in \mathbb{Q}[x]$

$$f_\alpha(pq) = f_\alpha(p)f_\alpha(q).$$

Now $f_\alpha(x^m x^n) = f_\alpha(x^{m+n}) = \alpha^{m+n} = \alpha^m\alpha^n = f_\alpha(x^m)f_\alpha(x^n)$. Thus the condition is satisfied by powers of x. It is also the case that

$$f_\alpha(ax^m) = a\alpha^m = f_\alpha(a)f_\alpha(x^m).$$

Putting this together with the solution to Exercise 4.7 shows that the required condition is satisfied in general.

Finally, we note that $f_\alpha(1) = 1$. Thus f_α is a homomorphism.

We are now in a position to show that, given an ideal $P = \langle p(x)\rangle$ in $\mathbb{Q}[x]$, we can find $\alpha \in \mathbb{C}$ such that P is equal to $\mathrm{Ker}(f_\alpha)$.

We mentioned the Fundamental Theorem of Algebra in Book C, Chapter 11, Section 4.1 (see the comments following Exercise 4.1). This theorem tells us that for any $p \in \mathbb{Q}[x]$ there is $\alpha \in \mathbb{C}$ such that α is a root of the polynomial equation $p(x) = 0$, that is

$$p(\alpha) = 0.$$

Since any element of P has the form pq for some $q \in \mathbb{Q}[x]$, and since

$$f_\alpha(pq) = p(\alpha)q(\alpha) = 0,$$

this means that $P \subseteq \mathrm{Ker}(f_\alpha)$. Our aim is to show that this inclusion is in fact an equality. For this, it will help to consider certain special ideals in the more general context of PIDs.

Definition 4.20 *Maximal ideal*

A proper ideal I of a ring R is a **maximal ideal** if whenever J is an ideal of R such that $I \subseteq J \subseteq R$, then either $I = J$ or $J = R$.

For example, $6\mathbb{Z}$ is not a maximal ideal of $\mathbb{Z}$ because it is a proper subset of the proper ideal $3\mathbb{Z}$. By contrast, if $p \in \mathbb{Z}$ is prime, then $p\mathbb{Z}$ is maximal. This is because by Lemma 2.7 any ideal I that contains $p\mathbb{Z}$ must be generated by a divisor of p, so either $I = p\mathbb{Z}$ or $I = 1\mathbb{Z} = \mathbb{Z}$.

Worked Exercise 4.21

Decide whether each of the following ideals of $\mathbb{Q}[x]$ is maximal.

(a) $\langle x^5 + x^4 + x^2 - 1\rangle$

(b) $\langle x^5 - 6x^2 + 9x + 6\rangle$

Solution

(a) The generator $x^5 + x^4 + x^2 - 1$ has -1 as one of its roots, and therefore has $x + 1$ as a proper factor. So $\langle x^5 + x^4 + x^2 - 1\rangle$ is not a maximal ideal because it is a proper subset of the ideal $\langle x + 1\rangle \neq \mathbb{Q}[x]$.

(b) Eisenstein's Criterion (Book C, Chapter 11, Theorem 4.15) for $p = 3$ tells us that $q(x) = x^5 - 6x^2 + 9x + 6$ is irreducible. Suppose that $\langle q(x)\rangle \subseteq I$ for some ideal I of $\mathbb{Q}[x]$. Since $\mathbb{Q}[x]$ is a PID, $I = \langle r(x)\rangle$ for some $r(x)$, and because $q(x)$ is irreducible, $r(x)$ is either a unit or an associate of $q(x)$. If $r(x)$ is a unit, then $\langle r(x)\rangle = \mathbb{Q}[x]$ by Exercise 2.4. If $r(x)$ is an associate of $q(x)$, then $\langle r(x)\rangle = \langle q(x)\rangle$ by Exercise 2.9. Therefore $\langle x^5 - 6x^2 + 9x + 6\rangle$ is a maximal ideal.

The above examples suggest that irreducible elements are the only elements capable of generating maximal ideals of a PID. The following theorem confirms that this is indeed the case.

Theorem 4.22

Let R be a PID, and let a be a non-zero, non-unit element of R. Then $\langle a\rangle$ is a maximal ideal of R if, and only if, a is irreducible in R.

Proof Let a be an irreducible element of R, and let $\langle b\rangle$ be an arbitrary ideal of R such that $\langle a\rangle \subset \langle b\rangle$. Then Lemma 2.7 implies that $a = bc$ for some $c \in R$. Since a is irreducible, either b is a unit, and hence by Exercise 2.4, $\langle b\rangle = R$, or c is a unit, and hence a and b are associates and so, by Exercise 2.9, $\langle a\rangle = \langle b\rangle$. So $\langle a\rangle$ is a maximal ideal.

Conversely, suppose $\langle a\rangle$ is maximal, and let $a = bc$. Then $\langle a\rangle \subseteq \langle b\rangle$. Since $\langle a\rangle$ is maximal, either $\langle b\rangle = \langle a\rangle$, in which case c is a unit by Lemma 2.7, or $\langle b\rangle = R$, in which case b is a unit. So a is irreducible. ■

Exercise 4.8

Which ideals are maximal in $\mathbb{Z}$?

We now return to our discussion about an irreducible polynomial $p(x) \in \mathbb{Q}[x]$. We had chosen $\alpha \in \mathbb{C}$ so that $p(\alpha) = 0$ and established that $\langle p\rangle \subseteq \mathrm{Ker}(f_\alpha)$ for the evaluation map f_α. We know that $\mathrm{Ker}(f_\alpha) \neq \mathbb{Q}[x]$. Theorem 4.22 also tells us that $\langle p\rangle$ is a maximal ideal. This means that $\langle p\rangle = \mathrm{Ker}(f_\alpha)$, and so

$$\mathbb{Q}[x]/\langle p\rangle \cong \mathrm{Im}\, f_\alpha.$$

So now we can explain the similarity between $\mathbb{Q}[x]/\langle x^2+1\rangle$ and $\mathbb{Q}[i]$ that we noticed in the comments following Exercise 4.6. We know that x^2+1 is irreducible in $\mathbb{Q}[x]$, and we know that i is a root of x^2+1 in $\mathbb{C}$. By the above discussion, we have that $\langle x^2+1\rangle$ is the kernel of the evaluation homomorphism f_i, and so

$$\mathbb{Q}[x]/\langle x^2+1\rangle \cong \mathrm{Im}(f_i).$$

But $\mathrm{Im}(f_i) = \{p(i) : p(x) \in \mathbb{Q}[x]\}$, and you can check that $\{p(i) : p(x) \in \mathbb{Q}[x]\} = \mathbb{Q}[i]$. Then

$$\mathbb{Q}[x]/\langle x^2+1\rangle \cong \mathbb{Q}[i]$$

so the 'similarity' is in fact an isomorphism.

The next theorem shows that the quotient rings formed from maximal ideals – that is, those generated by irreducible elements – are the only ones that are fields. It is worth noting that this result holds in arbitrary (commutative) rings, not just in PIDs.

Theorem 4.23

Let I be an ideal of a ring R. Then I is a maximal ideal if, and only if, R/I is a field.

Proof Suppose R/I is a field. Let J be an ideal of R containing I as a proper subset. Then there exists $a \in J$ such that $a \notin I$, and so $a+I$ is a non-zero element of R/I. Since R/I is a field there must be an element $b+I \in R/I$ such that $(a+I)(b+I) = ab+I = 1+I$. Then $1 \in ab+I \subseteq J$, and hence $J = R$. So I is a maximal ideal.

Conversely, suppose I is a maximal ideal of R. To show that R/I is a field we need to check that each of its non-zero elements has an inverse. Note that by 'non-zero' we mean 'different from the additive identity in R/I', that is, different from I. So let $a+I$ be a non-zero element of R/I.

Then $a \notin I$ so the ideal $J = I + \langle a\rangle = \{k+ar : k \in I, r \in R\}$ contains I as a proper subset. Since I is maximal, $J = R$, so $1 \in J$ and hence $1 = k+ar$ for some $r \in R$. Then $1-ar = k \in I$, so $ar+I = 1+I$, that is, $(a+I)(r+I) = 1+I$. It follows that $a+I$ has inverse $r+I$, and hence that R/I is a field. ■

Worked Exercise 4.24

Let $R = \mathbb{Z}_3[x]$, the ring of polynomials over $\mathbb{Z}_3$.

(a) Show that the polynomial x^2+1 is irreducible in R.

(b) Describe the quotient ring $R/\langle x^2+1\rangle$.

Solution

(a) Since $-1 = 2 \pmod 3$, there is no $x \in \mathbb{Z}_3$ such that $x^2 = -1$, that is, $x^2 + 1$ has no root in $\mathbb{Z}_3$. By the Factor Theorem (Book C, Chapter 11, Theorem 4.2), this implies that $x^2 + 1$ is irreducible in $\mathbb{Z}_3$.

(b) Since $x^2 + 1$ is irreducible and R is a Euclidean domain, and so a PID, $\langle x^2 + 1 \rangle$ is a maximal ideal. This means $R/\langle x^2 + 1 \rangle$ is a field.

Exercise 4.9

For each of the following values of $p(x)$, determine whether $p(x)$ is irreducible in $\mathbb{Z}_2[x]$. Hence determine whether $\mathbb{Z}_2[x]/\langle p(x) \rangle$ is a field.

(a) $p(x) = x^2 + 1$

(b) $p(x) = x^2 + x + 1$

4.5 Prime ideals

In the previous subsection we have seen that if M is a maximal ideal in a ring R then the quotient ring R/M is a field, and that in a PID irreducible elements generate maximal ideals. Since a PID is an integral domain, and since we know from Book C, Chapter 12, Theorem 2.12 that in an integral domain prime elements are irreducible, we now know that in a PID prime elements generate maximal ideals.

However, there are rings that are integral domains and not PIDs. A familiar example is the ring of polynomials over the integers, $\mathbb{Z}[x]$. Can we say anything about ideals generated by a prime element in such rings? It turns out that we can, but in order to do so we need to introduce the notion of a *prime ideal*.

Definition 4.25 *Prime ideal*

A proper ideal, P, in a ring R is **prime** if whenever $a, b \in R$ are such that $ab \in P$, then either $a \in P$ or $b \in P$.

In the next exercise you are asked to show that an ideal generated by a prime element is prime, and then to identify the prime ideals in $\mathbb{Z}$.

Exercise 4.10

(a) Let R be a ring. Show that, if $p \in R$ is a prime element, then the ideal $\langle p \rangle$ in R is a prime ideal.

(b) What are the prime ideals in $\mathbb{Z}$?

Just as quotient rings of maximal ideals are special, so are quotient rings of prime ideals.

Theorem 4.26

Let R be a commutative ring and P be an ideal of R. Then P is a prime ideal if, and only if, R/P is an integral domain.

Proof Suppose that P is a prime ideal of R and let $a + P, b + P \in R/P$ be such that

$$(a + P)(b + P) = P, \text{ the zero element of } R/P.$$

Then $ab + P = P$, so $ab \in P$. But P is prime, hence either $a \in P$ or $b \in P$. It follows that either $a + P = P$ or $b + P = P$, and P is the zero element of R/P. Therefore R/P is an integral domain.

Conversely, suppose that R/P is an integral domain and let $a, b \in R$ be such that $ab \in P$. Then $ab + P = P$, the zero element of R/P. Since R/P is an integral domain, either $a + P = P$ or $b + P = P$, that is, either $a \in P$ or $b \in P$. Therefore P is a prime ideal, as required. ■

In the next exercise, you are asked to show that in any ring maximal ideals are prime, but that the converse is not always true.

Exercise 4.11

(a) Let R be a ring and let I be a maximal ideal of R. Show that I is a prime ideal of R.

(b) Give an example of an ideal of $\mathbb{Z}[x]$ that is prime but not maximal.

Hint: for part (b), consider a prime ideal in $\mathbb{Z}$.

Under the stronger assumption that the ring is a PID, the converse to the statement in Exercise 4.11(a) is true.

Proposition 4.27

Let R be a PID and let P be a proper non-trivial ideal. If P is prime then:

(a) $P = \langle p \rangle$ for some prime element $p \in P$

(b) P is maximal in R.

Proof

(a) Since R is a PID, $P = \langle p \rangle$ for some $p \in P$. We need to show that p is a prime element of R. Suppose that $p \mid ab$ for some $a, b \in R$. Then $ab \in P$ by Lemma 2.7. But P is a prime ideal, so either $a \in P$ or $b \in P$. Again by Lemma 2.7, either $p \mid a$ or $p \mid b$. This shows that p is prime in R.

(b) From part (a), $P = \langle p \rangle$ for a prime element p of R. Since R is an integral domain, p is irreducible in R by Theorem 2.12 of Book C, Chapter 12. Then P is maximal by Theorem 4.22. ■

If the ring is a UFD, prime ideals are not necessarily maximal, but we can still say something useful.

Lemma 4.28

Let P be a prime ideal in a ring R. Then if $a_1 a_2 \cdots a_n \in P$ there is an $i \in \{1, \ldots, n\}$ with $a_i \in P$.

Proof We use induction on n. The result is true for $n = 2$ by the definition of a prime ideal. Suppose that it is true for $n = k$ and suppose that $a_1 \cdots a_k a_{k+1} \in P$. Then let $b = a_1 \cdots a_k$ so that $b a_{k+1} \in P$. By the definition of a prime ideal, either $b \in P$ or $a_{k+1} \in P$. If $b \in P$, by the induction hypothesis there is an $a_i \in P$ for $i \in \{1, \ldots, k\}$. Thus there is an $i \in \{1, \ldots, k+1\}$ with $a_i \in P$. The result follows by induction. ■

Proposition 4.29

Let R be a UFD and suppose that P is a non-zero prime ideal in R. Then P contains an irreducible element q.

Proof Let $a \in P$. Since R is a UFD we can write $a = u p_1 p_2 \cdots p_n$ where u is a unit and p_i is an irreducible element of R for $i = 1, \ldots, n$. Then $p_1 p_2 \cdots p_n \in P$. Since P is a prime ideal, Lemma 4.28 gives an $i \in \{1, \ldots, n\}$ such that $p_i \in P$. ■

In the next exercise you are asked to prove a property of prime ideals in a UFD where every prime ideal is maximal.

Exercise 4.12

Let R be a UFD in which every prime ideal is maximal. Let P be a prime ideal in R. Show that $P = \langle q \rangle$ for some irreducible element q in R.

Identifying prime ideals in a commutative ring is often a first step in understanding the ring. In the last exercise of this chapter you are asked to do this for two familiar polynomial rings.

We know from Theorem 3.1 of Book C, Chapter 11 that if K is a field then the polynomial ring $K[x]$ is a Euclidean domain, and hence a PID. Therefore we can apply Proposition 4.27 and conclude that all non-zero prime ideals in $K[x]$ are of the form $\langle p(x) \rangle$, where $p(x)$ is an irreducible polynomial. Furthermore, these ideals are maximal.

Exercise 4.13

Describe the non-zero prime ideals in

(a) $\mathbb{C}[x]$

(b) $\mathbb{R}[x]$.

Learning outcomes

We list those topics on which we may set assessment questions to test your understanding of the chapter.

After working through this chapter you should be able to:

(a) Understand how to find the field of fractions of an integral domain.

(b) Decide whether a given set is an ideal of a ring.

(c) In simple cases show that a given ideal is not a principal ideal.

(d) Find the highest common factor of elements in a Euclidean domain, using the Euclidean Algorithm.

(e) In simple cases determine whether or not a ring is a PID.

(f) Carry out calculations involving sums and products of ideals.

(g) Describe the set of cosets of $\mathbb{Q}[x]/I$ for a given principal ideal I.

(h) Identify the image and kernel of a homomorphism.

(i) Determine whether a given ideal is a maximal ideal.

(j) Determine whether a given ideal is a prime ideal.

Solutions to exercises

Solution to Exercise 1.1

Since multiplication in D is commutative, for any a and b in D we have that $ab = ba$, and so $(a, b) \sim (a, b)$.

The commutativity of multiplication in D also implies that if $ad = bc$ then $cb = da$. This shows that if $(a, b) \sim (c, d)$ then $(c, d) \sim (a, b)$, that is, $\sim$ is symmetric.

Solution to Exercise 1.2

We have to show that if $[a, b] = [a_1, b_1]$ and $[c, d] = [c_1 d_1]$, then $[ac, bd] = [a_1c_1, b_1d_1]$, that is,

$$(ac, bd) \sim (a_1c_1, b_1d_1).$$

So we need to show that

$$(ac)(b_1d_1) = (bd)(a_1c_1).$$

This follows directly from equation $(*)$.

Solution to Exercise 1.3

(a) The common denominator of the coefficients of the polynomial on the left-hand side is 30, so

$$\frac{1}{2} + \frac{2}{3}x + \frac{1}{5}x^3 = \frac{1}{30}\left(15 + 20x + 6x^3\right).$$

(b) Let $q(x) = q_0 + q_1x + \cdots + q_nx^n$. Then for each i from $0, \ldots, n$ we can write $q_i = \frac{c_i}{d_i}$ where $c_i, d_i \in R$ and $d_i \neq 0$. Let d be the product $d_0d_1 \cdots d_n$. Then $p_i = q_id \in R$. Thus $dq(x) = p(x) \in R[x]$ and so $q(x) = \frac{1}{d}p(x)$. The result follows with $f = \frac{1}{d}$.

Solution to Exercise 1.4

By Proposition 4.7 of Book C, Chapter 12, $\mathrm{hcf}(a, b) = h$, where h is the product of those irreducible elements that occur in both the factorisations of a and of b. (We may assume that the irreducible factors are the same by multiplying by suitable units if necessary.)

Then $a = hc$ and $b = hd$, where c and d have no common irreducible factors, and so $\mathrm{hcf}(c, d) = u$, where u is a unit. Moreover, by Lemma 1.2(a) $\frac{a}{b} = \frac{c}{d}$, as required.

Solution to Exercise 1.5

(a) We use induction on n. The case $n = 2$ is proved in the solution to Exercise 4.1 of Book C, Chapter 12. We now assume that the result holds for $n = k$, that is, we assume that $\text{lcm}(b_1, b_2, \ldots, b_k)$ exists. Let $l_k = \text{lcm}(b_1, b_2, \ldots, b_k)$. Then, again by the solution to Exercise 4.1 in Chapter 12, $l_{k+1} = \text{lcm}(l_k, b_{k+1})$ exists. We now show that $l_{k+1} = \text{lcm}(b_1, b_2, \ldots, b_{k+1})$.

(i) $l_{k+1} = l_k r$ and $l_{k+1} = b_{k+1} d_{k+1}$ for some $r, d_{k+1} \in D$. By the induction hypothesis $l = b_i d_i$ for some $d_i \in D, i = 1, \ldots, n$. Thus $l_{k+1} = b_i(d_i r), i = 1, \ldots, n$.

(ii) Suppose that $d = b_i d_i$ for some $d_i, i = 1, \ldots, k+1$. Then by the induction hypothesis $d = ls$ for some $s \in D$ and so by the solution to Exercise 4.1 of Chapter 12, $d = l_{k+1} t$ for some $t \in D$.

We have shown that $l_{k+1} = \text{lcm}(b_1, b_2, \ldots, b_{k+1})$. The result follows by induction.

(b) Let $b = \text{lcm}(b_1, b_2, \ldots, b_n)$, so that $b = b_i c_i$ for some $c_i, i = 1, \ldots, n$. Then

$$\frac{a_i}{b_i} = \frac{a_i c_i}{b_i c_i} = \frac{a_i c_i}{b}$$

as required.

Solution to Exercise 2.1

By I2, $-b = (-1)b \in I$, and so, by I1, $a + b = a - (-b) \in I$.

Solution to Exercise 2.2

The set K is non-empty, since $0 \in K$. Moreover,

I1 if $u, v \in K$, then $(u - v)r = ur - vr = 0 - 0 = 0$, so $u - v \in K$;

I2 if $u \in K$ and $s \in R$, then $ur = 0$ and $(su)r = s(ur) = 0$, so $su \in K$.

Therefore K is an ideal of R.

Solution to Exercise 2.3

We first observe that $0 = q \cdot 0 \in q\mathbb{Q}[x]$, so $q\mathbb{Q}[x]$ is non-empty.
Next we check the ideal conditions.

I1 Let qk_1 and qk_2 be two arbitrary elements of $q\mathbb{Q}[x]$. Then

$$qk_1 - qk_2 = q(k_1 - k_2) \in q\mathbb{Q}[x].$$

I2 Let qk be an arbitrary element of $q\mathbb{Q}[x]$ and let $r \in \mathbb{Q}[x]$. Then

$$r(qk) = q(rk) \in q\mathbb{Q}[x].$$

We conclude that $q\mathbb{Q}[x]$ is an ideal of $\mathbb{Q}[x]$.

Solution to Exercise 2.4

Since u is a unit in R, there is an element $u^{-1} \in R$ such that $uu^{-1} = 1$. Hence $1 \in \langle u \rangle$ and so if $r \in R$, by I2, $r = 1 \cdot r \in \langle u \rangle$. Thus $\langle u \rangle = R$.

Solution to Exercise 2.5

Suppose that F is a field and that I is a non-trivial ideal in F. Let $a \in I$ with $a \neq 0$. Then, since F is a field, $a^{-1} \in F$ and so, by I2, $1 = aa^{-1} \in I$, which implies that $I = F$. Thus F contains no proper non-trivial ideals.

Now suppose that F contains no proper non-trivial ideals. Let $a \in F$ with $a \neq 0$ and consider the ideal $\langle a \rangle$. Since F contains no proper non-trivial ideals, and since $a \neq 0$, we have that $\langle a \rangle = F$ and so $1 \in \langle a \rangle$. This implies there is $r \in F$ with $ar = 1$, that is, $r = a^{-1} \in F$. Hence every non-zero element of F has a multiplicative inverse, and so F is a field as required.

Solution to Exercise 2.6

(a) We check the subring criterion (Book C, Chapter 11, Lemma 1.8).

Since $0 = 0 + 0\alpha$, T contains 0 and so it is non-empty. Let $a + b\alpha, c + d\alpha \in T$, where $a, b, c, d \in R$. Then

SR1 $(a + b\alpha) - (c + d\alpha) = (a - c) + (b - d)\alpha \in T$, because R is a subring of S, and so $a - c$ and $b - d$ are elements of R;

SR2
$$\begin{aligned}(a + b\alpha)(c + d\alpha) &= ac + bd\alpha^2 + (ad + bc)\alpha \\ &= ac + bdr + (ad + bc)\alpha \in T,\end{aligned}$$
since R is a subring of S;

SR3 $1 = 1 + 0\alpha \in T$, so T contains the multiplicative identity 1.

It follows that T is a subring of S.

(b) We need to show that T is the smallest subring of S that contains both R and α. Because of the way it has been defined, T does contain both R and α. Suppose that W is a subring that contains both R and α. If $a, b \in R$ then $a + b\alpha \in W$ by the additive and multiplicative closure of W. Therefore every element of T is an element of W, and so $T \subseteq W$. Hence T is indeed the smallest subring of S that contains both R and α.

Solution to Exercise 2.7

(a) Since $(1 + \sqrt{2})(-1 + \sqrt{2}) = 1$, the element $1 + \sqrt{2}$ is a unit, hence $\langle 1 + \sqrt{2} \rangle = R$ by Exercise 2.4.

(b) Since $1 \neq 2a$ for all $a \in \mathbb{Z}$, $1 \notin \langle 2 \rangle = \{2a\}$. Then $\langle 2 \rangle \neq R$.

Solution to Exercise 2.8

First suppose that $aR \subseteq bR$. Then $a = a \cdot 1 \in aR \subseteq bR$, so $a = rb$ for some $r \in R$. That is, $b \mid a$.

Conversely, suppose $b \mid a$. Then there is an $s \in R$ such that $a = bs$. Now let $ar \in aR$. Then

$$ar = (bs)r = b(sr) \in bR.$$

Therefore $aR \subseteq bR$.

Solution to Exercise 2.9

By Lemma 2.7, $aR = bR$ if, and only if, $b \mid a$ and $a \mid b$.

Now, if $b \mid a$ and $a \mid b$, then a and b are associates by Lemma 2.13(b) of Book C, Chapter 12.

On the other hand, if a and b are associates, then $a = ub$ for some unit u, and $b = u^{-1}a$, so $b \mid a$ and $a \mid b$. It follows that each of aR and bR contain the other, and hence $aR = bR$.

So $aR = bR$ if, and only if, a and b are associates.

Solution to Exercise 2.10

The zero element is a member of I_0 and therefore a member of I, so I is non-empty. Also:

I1 If $a, b \in I$, then $a \in I_i$ and $b \in I_j$ for some integers $i, j \geq 0$, so $a, b \in I_k$ where $k = \max(i, j)$. Since I_k is an ideal, we have $a - b \in I_k \subseteq I$.

I2 If $a \in I$ and $r \in R$, then $a \in I_i$ for some integer $i \geq 0$. Since I_i is an ideal we have $ra \in I_i \subseteq I$.

Hence I is an ideal of R.

Solution to Exercise 2.11

(a) Since $0 \in I_1$ and $0 \in I_2$, the intersection $I_1 \cap I_2$ contains 0, and so it is non-empty. Moreover:

I1 If $a, b \in I_1 \cap I_2$, then $a - b \in I_1$ because I_1 is an ideal, and $a - b \in I_2$ because I_2 is an ideal, so $a - b \in I_1 \cap I_2$.

I2 If $a \in I_1 \cap I_2$ and $r \in R$, then $ar \in I_1$ because I_1 is an ideal of R, and $ar \in I_2$ because I_2 is an ideal of R, so $ar \in I_1 \cap I_2$, as required.

It follows that $I_1 \cap I_2$ is an ideal of R.

(b) Clearly $2 \in 2\mathbb{Z}$ and $7 \in 7\mathbb{Z}$, but $2 - 7 = -5$ is neither a multiple of 2 nor of 7, so $-5 \notin 2\mathbb{Z} \cup 7\mathbb{Z}$. Hence $2\mathbb{Z} \cup 7\mathbb{Z}$ is not closed under subtraction and therefore it is not an ideal of $\mathbb{Z}$.

Solution to Exercise 2.12

A highest common factor exists because $\mathbb{Z}[\sqrt{-2}]$ is a Euclidean domain, and hence a PID, so we can use the Euclidean Algorithm to find the hcf.

We begin by using ordinary complex division to divide the number with larger norm by the number with smaller norm:

Multiply the numerator and the denominator by $(1 - 5\sqrt{-2})$.

$$\frac{9 + 11\sqrt{-2}}{1 + 5\sqrt{-2}} = \frac{119 - 34\sqrt{-2}}{51} = (2 - \sqrt{-2}) + \tfrac{1}{3}(1 + \sqrt{-2}),$$

where $(2 - \sqrt{-2})$ is the element of $\mathbb{Z}[\sqrt{-2}]$ whose Euclidean norm is closest to that of $\frac{1}{51}(119 - 34\sqrt{-2})$. Then multiplying through by $1 + 5\sqrt{-2}$ gives the quotient–remainder form

$$9 + 11\sqrt{-2} = (2 - \sqrt{-2})(1 + 5\sqrt{-2}) + (-3 + 2\sqrt{-2}).$$

Since the remainder $(-3+2\sqrt{-2})$ is still non-zero, we calculate

$$\frac{1+5\sqrt{-2}}{-3+2\sqrt{-2}} = \frac{17-17\sqrt{-2}}{17} = 1-\sqrt{-2} \in \mathbb{Z}[\sqrt{-2}].$$

The remainder is now zero, so the hcf is the previous remainder:

$$\text{hcf}(9+11\sqrt{-2}, 1+5\sqrt{-2}) = -3+2\sqrt{-2}.$$

Solution to Exercise 2.13

(a) You saw in the solution to Exercise 3.1 of Book C, Chapter 12, that $\mathbb{Z}[\sqrt{-2}]$ is a Euclidean domain, so by Theorem 2.11 it must also be a PID.

(b) If $\mathbb{Z}[\sqrt{-5}]$ were a PID then, by Theorem 2.16, it would also be a UFD. However, we know that $\mathbb{Z}[\sqrt{-5}]$ is not a UFD: for example,

$$6 = 3 \cdot 2 = (1+\sqrt{-5}) \cdot (1-\sqrt{-5})$$

exhibits two different factorisations into irreducibles, as shown in the solution to Exercise 2.6(d) of Book C, Chapter 12. Therefore we conclude that $\mathbb{Z}[\sqrt{-5}]$ is not a PID.

Solution to Exercise 3.1

If $a \in A$ then $a = a + 0 \in A + B$, and so $A \subseteq (A+B)$.
Similarly, if $b \in B$, then $b = 0 + b \in A + B$, and so $B \subseteq (A+B)$.

Solution to Exercise 3.2

Let $x \in \langle a \rangle + \langle b \rangle$. Then $x = sa + tb$ for some $s, t \in R$. Since $h \mid a$ and $h \mid b$, we have that $h \mid x$, and hence $x \in \langle h \rangle$ by Lemma 2.7.

Conversely, if $x \in \langle h \rangle$, then $x = rh$ for some $r \in R$. By Theorem 2.13, there exist $s, t \in R$ such that $h = sa + tb$, so

$$x = rh = (rs)a + (rt)b \in \langle a \rangle + \langle b \rangle.$$

It follows that $\langle a \rangle + \langle b \rangle = \langle h \rangle$.

Solution to Exercise 3.3

Since $0 = 0 \cdot 0 \in AB$, AB is non-empty, so we are left to check the ideal conditions.

I1 Let $a_1b_1 + \cdots + a_kb_k$ and
$c_1d_1 + \cdots + c_\ell d_\ell$
be two arbitrary elements of AB. Then their difference is equal to

$$a_1b_1 + \cdots + a_kb_k + (-c_1)d_1 + \cdots + (-c_\ell)d_\ell,$$

which is an element of AB by the way AB has been defined.

I2 Let $a_1b_1 + \cdots + a_kb_k \in AB$ and let $r \in R$. Then

$$r(a_1b_1 + \cdots + a_kb_k) = (ra_1)b_1 + \cdots + (ra_k)b_k \in AB,$$

where I2 for A ensures that each $ra_i \in A$.

Hence AB is an ideal.

Solution to Exercise 3.4

(a) The ideal $\langle 27, 36\rangle$ must be principal because $\mathbb{Z}$ is a PID.

So let h be a generator of $\langle 27, 36\rangle$. Then h is a common factor of every element of $\langle 27, 36\rangle$, and in particular of 27 and 36. But $h \in \langle 27, 36\rangle$ so $h = 27a + 36b$ for some $a, b \in \mathbb{Z}$. Therefore every common factor of 27 and 36 is also a factor of h. In other words, $h = \text{hcf}(27, 36) = 9$.

Alternatively, since $\langle 27, 36\rangle$ is equal to $\langle 27\rangle + \langle 36\rangle$, by the solution to Exercise 3.2 the generator must be equal to $\text{hcf}(27, 36) = 9$.

(b) The ideal $\langle x, 2\rangle$ is not principal. In fact, we claim it is the ideal A of polynomials in $\mathbb{Z}[x]$ with even constant terms, which we showed to be non-principal in the solution to Worked Exercise 2.12. So it is sufficient to prove that $\langle x, 2\rangle = A$.

Since both 2 and x have an even constant term, they are both elements of A. The closure properties of A then ensure that $\langle x, 2\rangle \subseteq A$.

Conversely, every polynomial in A has an even constant term, and therefore has the form

$$2a + x(a_1 + a_2x + \cdots + a_nx^{n-1}) \in \langle x, 2\rangle,$$

so $A \subseteq \langle x, 2\rangle$. Thus $A = \langle x, 2\rangle$, as required.

Solution to Exercise 3.5

(a) Since $\mathbb{Z}[i]$ is a Euclidean domain, A must be a principal ideal generated by $\text{hcf}(3 + i, 1 + 3i)$. In the solution to Exercise 2.14 it was shown that $\text{hcf}(3 + i, 1 + 3i) = (-1 - i)$, so $A = \langle -1 - i\rangle$.

(b) The ring $\mathbb{Z}[\sqrt{-5}]$ is not a PID, so A might not be principal. We will use the multiplicative norm $N(a + b\sqrt{-5}) = a^2 + 5b^2$ to prove that it is not principal.

Suppose A is generated by some element $t \in A$. We know that $2 \in A$ and $(1 + \sqrt{-5}) \in A$, so $2 = rt$ and $(1 + \sqrt{-5}) = st$ for some $r, s \in \mathbb{Z}[\sqrt{-5}]$.

Taking norms shows that $N(t)$ must be a factor of both $N(2) = 4$ and $N(1 + \sqrt{-5}) = 6$. So either $N(t) = 2$ or $N(t) = 1$. But $N(u + v\sqrt{-5}) = u^2 + 5v^2 = 2$ has no integer solutions, and the only integer solutions of $u^2 + 5v^2 = 1$ are $u = \pm 1$ with $v = 0$, so $t = \pm 1$. But if this value of t really does lie in A, then there are integers a, b, c, d such that

$$\begin{aligned}\pm 1 &= 2(a + b\sqrt{-5}) + (1 + \sqrt{-5})(c + d\sqrt{-5})\\ &= (2a + c - 5d) + (2b + c + d)\sqrt{-5}.\end{aligned}$$

But this implies $2b + c + d = 0$, and hence $c = -2b - d$. So

$$\pm 1 = 2a + c - 5d = 2a - 2b - 6d.$$

But the right-hand side is even, which is a contradiction.

Therefore the assumption that A is generated by t must be false, and so A is not principal.

Solution to Exercise 3.6

(a) Since $x^2 - 1 = (x+1)(x-1) \in \langle x-1 \rangle$ and $x^2 - 2x + 1 = (x-1)^2 \in \langle x-1 \rangle$, we have $\langle x^2-1, x^2-2x+1 \rangle \subseteq \langle x-1 \rangle$ by Proposition 3.8. In fact, the ideal $\langle x^2-1, x^2-2x+1 \rangle$ is a *proper* subset of the ideal $\langle x-1 \rangle$ but this is a bit tricky to show.

(b) (i) We have $(1+\sqrt{-5}) = 2 - (1-\sqrt{-5})$. Hence

$$1 + \sqrt{-5} \in \langle 2, 1 - \sqrt{-5} \rangle,$$

and so $\langle 2, 1+\sqrt{-5} \rangle \subseteq \langle 2, 1-\sqrt{-5} \rangle$ by Proposition 3.8.

Similarly, since $(1-\sqrt{-5}) = 2 - (1+\sqrt{-5})$ we have that

$$\langle 2, 1-\sqrt{-5} \rangle \subseteq \langle 2, 1+\sqrt{-5} \rangle.$$

Hence $\langle 2, 1+\sqrt{-5} \rangle = \langle 2, 1-\sqrt{-5} \rangle$, as required.

(ii) Since $\langle 2-\sqrt{-5} \rangle$ is closed under multiplication by elements of $\mathbb{Z}[\sqrt{-5}]$, and in particular by the element $2+\sqrt{-5}$, we have

$$(2+\sqrt{-5})(2-\sqrt{-5}) = 9 \in \langle 2-\sqrt{-5} \rangle.$$

Hence $\langle 9 \rangle \subseteq \langle 2-\sqrt{-5} \rangle$ by Proposition 3.8.

Solution to Exercise 3.7

First we note that $\langle I, t \rangle$ is non-empty, since $t \in \langle I, t \rangle$. Moreover:

I1 Let $b_1, b_2 \in R$ and $m_1, m_2 \in I$. Then

$$(m_1 + b_1 t) - (m_2 + b_2 t) = (m_1 - m_2) + (b_1 - b_2)t.$$

Since I is an ideal, $m_1 - m_2 \in I$, and so $(m_1 - m_2) + (b_1 - b_2)t \in \langle I, t \rangle$.

I2 Let $b, r \in R$ and $m \in I$. Then

$$(m + bt)r = mr + btr.$$

Since I is an ideal, $mr \in I$. Since R is commutative, $btr = brt$, and so $(mr + btr) \in \langle I, t \rangle$.

Solution to Exercise 4.1

Let $a+I$, $b+I$, $c+I$ be arbitrary cosets of I by a, b, c, respectively.

The set of cosets with addition, $(S, +)$, is a quotient group of an abelian group, and so it is itself an abelian group. We need to show the remaining axioms of a commutative ring are satisfied. In what follows, we will, as usual, replace $\cdot$ by juxtaposition.

Axioms for multiplication

R6 Closure The closure of $\cdot$ is immediate from the definition because $(ab) + I$ is clearly a coset.

R7 Associativity We have

$$\begin{aligned}(a+I)((b+I)(c+I)) &= a(bc) + I \\ &= (ab)c + I \\ &= ((a+I)(b+I))(c+I).\end{aligned}$$

R8 Multiplicative identity The multiplicative identity is $1 + I$, for

$$(1 + I)(a + I) = 1a + I = a + I.$$

R9 Distributive laws For left distributivity, we have

$$\begin{aligned}(a + I)\left((b + I) + (c + I)\right) &= a(b + c) + I \\ &= (ab + ac) + I \\ &= (ab + I) + (ac + I) \\ &= (a + I)(b + I) + (a + I)(c + I),\end{aligned}$$

so distributivity in S follows from distributivity in R. Right distributivity follows from commutativity in R.

R10 Commutativity

$$\begin{aligned}(a + I)(b + I) &= ab + I \\ &= ba + I \\ &= (b + I)(a + I)\end{aligned}$$

The ring axioms R1–R9 hold for S even when R is not commutative. Only right distributivity needs to be checked in addition to the above, and this is similar to left distributivity.

Solution to Exercise 4.2

(a) Each coset has the form $f(x) + I$, where $f \in \mathbb{Q}[x]$. By the Division Algorithm, we can write

$$f(x) = q(x)(x^2 + x + 1) + r(x),$$

where $q, r \in \mathbb{Q}[x]$ with $\deg(r) < \deg(x^2 + x + 1) = 2$. So

$$f(x) - r(x) = q(x)(x^2 + x + 1) \in I.$$

By Proposition 4.2,

$$f(x) + I = r(x) + I.$$

But $\deg(r) < 2$, so $r(x)$ has the form $a + bx$, and

$$R/I = \{(a + bx) + I : a, b \in \mathbb{Q}\}.$$

(b) If $a + bx + I$ and $c + dx + I$ are arbitrary elements of R/I, then

$$\begin{aligned}(a + bx + I) + (c + dx + I) &= (a + bx) + (c + dx) + I \\ &= (a + c) + (b + d)x + I \quad \text{and} \\ (a + bx + I) \cdot (c + dx + I) &= (a + bx) \cdot (c + dx) + I \\ &= ac + (ad + bc)x + bdx^2 + I.\end{aligned}$$

Now $x^2 + x + 1 \in I$, so $x^2 + I = -x - 1 + I$. Then

$$\begin{aligned}ac + (ad + bc)x + bdx^2 + I &= ac + (ad + bc)x + bd(-x - 1) + I \\ &= (ac - bd) + (ad + bc - bd)x + I.\end{aligned}$$

Thus the formula for multiplication is

$$(a + bx + I)(c + dx + I) = (ac - bd) + (ad + bc - bd)x + I.$$

Solution to Exercise 4.3

(a) Let $r, s \in \mathbb{Z}[x]$. Then $f(1) = 1$,

$$\begin{aligned} f(r+s) &= (r+s)(0) \\ &= r(0) + s(0) \\ &\equiv f(r) + f(s) \pmod 2, \quad \text{and} \\ f(rs) &= rs(0) \\ &= r(0)s(0) \\ &\equiv f(r)f(s) \pmod 2, \end{aligned}$$

so f is a ring homomorphism.

(b) Let $a + b\sqrt{5}, c + d\sqrt{5} \in \mathbb{Q}[\sqrt{5}]$. Then $f(1) = 1$, and

$$\begin{aligned} f\left((a+b\sqrt{5}) + (c+d\sqrt{5})\right) &= f\left((a+c) + (b+d)\sqrt{5}\right) \\ &= (a+c) - (b+d)\sqrt{5} \\ &= (a - b\sqrt{5}) + (c - d\sqrt{5}) \\ &= f\left(a+b\sqrt{5}\right) + f\left(c+d\sqrt{5}\right), \end{aligned}$$

$$\begin{aligned} f\left((a+b\sqrt{5})(c+d\sqrt{5})\right) &= f\left((ac+5bd) + (ad+bc)\sqrt{5}\right) \\ &= (ac+5bd) - (ad+bc)\sqrt{5} \\ &= (a - b\sqrt{5})(c - d\sqrt{5}) \\ &= f\left(a+b\sqrt{5}\right) f\left(c+d\sqrt{5}\right), \end{aligned}$$

so f is a homomorphism.

(c) Let $a, b \in \mathbb{Z}$. Then $f(1) = 1$,

$$f(a+b) = a + b + 0i = (a+0i) + (b+0i) = f(a) + f(b), \text{ and}$$
$$f(ab) = ab + 0i = (a+0i)(b+0i) = f(a)f(b),$$

so f is a homomorphism.

Solution to Exercise 4.4

(a) Since $0_R + 0_R = 0_R$, we have

$$f(0_R) = f(0_R + 0_R) = f(0_R) + f(0_R).$$

Adding $-f(0_R)$ to both sides gives $0_S = f(0_R)$, as required.

(b) Since $a + (-a) = 0_R$, we have

$$0_S = f(0_R) = f(a + (-a)) = f(a) + f(-a).$$

But additive inverses are unique, so $f(-a) = -f(a)$, as required.

(c) If $u \in R$ is a unit, then $ur = 1$ for some $r \in R$. Then

$$1_S = f(1_R) = f(ur) = f(u)f(r).$$

So $f(u)$ is a unit, as required.

Solution to Exercise 4.5

(a) We have $f(0) = 0$ and $f(1) = 1$. So $\mathrm{Im}(f) = \mathbb{Z}_2$, and f is onto.

Now let $r \in \mathbb{Z}[x]$ be such that $f(r) = 0$, that is, such that $r(0) \equiv 0 \pmod 2$. Then the constant term of r is even. This shows that

$$\mathrm{Ker}(f) = \{a_0 + a_1x + \cdots + a_nx^n : a_0 \text{ is even}\},$$

and so f is not one–one.

(b) Let $c \in \mathbb{Z}[\sqrt{5}]$. Then $c = a + b\sqrt{5}$ for some $a, b \in \mathbb{Z}$, and so $c = f\left(a - b\sqrt{5}\right)$. Therefore $\mathrm{Im}(f) = \mathbb{Z}[\sqrt{5}]$, and f is onto.

Now let $f(a + b\sqrt{5}) = a - b\sqrt{5} = 0$. Then $a = b = 0$, and hence $a + b\sqrt{5} = 0$. So $\mathrm{Ker}(f) = \{0\}$ and f is one–one.

(c) Here $\mathrm{Im}(f) \neq \mathbb{C}$ since $i \notin \mathrm{Im}(f)$. So f is not onto. In fact, $\mathrm{Im}(f) = \{a + 0i : a \in \mathbb{Z}\}$.

Now let $0 + 0i = f(a) = a + 0i$. Then $a = 0$ and hence $\mathrm{Ker}(f) = \{0\}$. So f is one–one.

Solution to Exercise 4.6

We have $\hat{f}_p(a_0 + a_1x + \cdots + a_nx^n) = 0 + 0x + \cdots + 0x^n$ if, and only if, $a_i \equiv 0 \pmod p$ for $i = 1, 2, \ldots, n$. The latter condition holds if, and only if, each of the coefficients $a_0, a_1, \ldots, a_n$ is an integer multiple of p. So $\mathrm{Ker}(\hat{f}_p) = p\mathbb{Z}[x]$.

Solution to Exercise 4.7

Let $p(x) = a_0 + a_1x + \cdots + a_nx^n$ and $q(x) = b_0 + b_1x + \cdots + b_mx^m$. We assume without loss of generality that $m \geq n$. Then

$$\begin{aligned} f_\alpha(p + q) &= f_\alpha(a_0 + b_0 + (a_1 + b_1)x + \cdots + (a_n + b_n)x^n + b_{n+1}x^{n+1} + \cdots + b_mx^m) \\ &= a_0 + b_0 + (a_1 + b_1)\alpha + \cdots + (a_n + b_n)\alpha^n + b_{n+1}\alpha^{n+1} + \cdots + b_m\alpha^m \\ &= a_0 + a_1\alpha + \cdots + a_n\alpha^n + b_0 + b_1\alpha + \cdots + b_m\alpha^m \\ &= f_\alpha(p) + f_\alpha(q). \end{aligned}$$

Solution to Exercise 4.8

Since $\mathbb{Z}$ is a PID, we know from Theorem 4.22 that maximal ideals have the form $\langle p \rangle$ where p is an irreducible element, that is, an integer prime.

Solution to Exercise 4.9

(a) Since 1 is a root of $x^2 + 1$ in $\mathbb{Z}_2$, the Factor Theorem tells us that $x^2 + 1$ is reducible. In fact

$$x^2 + 1 \equiv x^2 + 2x + 1 \equiv (x + 1)(x + 1) \pmod 2.$$

Since $\mathbb{Z}_2[x]$ is a PID, $\langle x^2 + 1 \rangle$ is not a maximal ideal by Theorem 4.22, and so $\mathbb{Z}_2[x]/\langle x^2 + 1 \rangle$ is not a field by Theorem 4.23.

(b) If $p(x) = x^2 + x + 1$ is reducible over $\mathbb{Z}_2$, either $p(0) = 0$ or $p(1) = 0$ by the Factor Theorem. But $p(0) = p(1) = 1$, and so $p(x)$ is irreducible over $\mathbb{Z}_2$. Then $\mathbb{Z}_2[x]/\langle x^2 + x + 1 \rangle$ is a field.

Solution to Exercise 4.10

(a) Let $ab \in \langle p \rangle$, so that $ab = pr$ for some $r \in R$. So $p \mid ab$, and since the element p is prime in R, either $p \mid a$ or $p \mid b$. Without loss of generality we assume $p \mid a$, so there is $s \in R$ such that $ps = a$, which implies that $a \in \langle p \rangle$, as required.

(b) Since $\mathbb{Z}$ is a PID all its ideals are of the form $\langle a \rangle$. From part (a) we know that if a is a prime integer then $\langle a \rangle$ is a prime ideal. If a is non-zero and not prime, then $a = bc$ for some $b, c \neq 1$ so that $bc \in \langle a \rangle$ but $b \notin \langle a \rangle$ and $c \notin \langle a \rangle$. Thus the non-zero prime ideals of $\mathbb{Z}$ are all the ideals $\langle a \rangle$ where a is a prime integer. Since $\mathbb{Z}$ has no zero divisors, $\langle 0 \rangle$ is also a prime ideal in $\mathbb{Z}$.

Solution to Exercise 4.11

(a) Since I is maximal, by Theorem 4.23, R/I is a field and hence it is an integral domain. Hence I is prime by Theorem 4.26.

(b) The ideal $\langle 5 \rangle$ is prime in $\mathbb{Z}[x]$ by Lemma 4.10 of Book C, Chapter 12 and by the solution to Exercise 4.10(a). However, $\langle 5 \rangle$ is not maximal, since it is properly contained, say, in $\langle 5, x \rangle$, which in turn is properly contained in $\mathbb{Z}[x]$.

Solution to Exercise 4.12

By Proposition 4.29, since R is a UFD, P contains an irreducible element Q. Since R is a UFD, q is a prime element by Corollary 4.3 of Book C, Chapter 12. Thus $\langle q \rangle$ is a prime ideal by the solution to Exercise 4.10(a), and since $q \in P, \langle q \rangle \subseteq P$. Since every prime ideal is maximal, we must have $\langle q \rangle = P$ as required.

Solution to Exercise 4.13

(a) Irreducible polynomials in $\mathbb{C}[x]$ can all be written in the form $ax - b$, for some $a, b \in \mathbb{C}$ with $a \neq 0$, and so the non-zero prime ideals of $\mathbb{C}[x]$ are all the ideals $\langle x - c \rangle$ for some $c \in \mathbb{C}$ (we can divide $ax - b$ through by a as a is non-zero). The Fundamental Theorem of Algebra and the Factor Theorem tell us that there are no other irreducible polynomials in $\mathbb{C}[x]$, so there will be no other non-zero prime ideals.

(b) As for $\mathbb{C}[x]$, all the ideals of the form $\langle x - c \rangle$ for some $c \in \mathbb{R}$ are prime in $\mathbb{R}[x]$. In addition, ideals of the form

$$\langle x^2 + bx + c \rangle,$$

where $x^2 + bx + c$ is irreducible, are also prime. There are no other irreducible polynomials in $\mathbb{R}[x]$, and so there are no other non-zero prime ideals.

Chapter 18

Fields and polynomials

Introduction

In this chapter we embark on a systematic study of fields. As you know from Book C, fields are a special sort of ring – loosely, one in which division is possible by every element but zero. We have already met several examples of fields. In addition to the familiar number fields $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$, we worked with the finite field of p elements, where p is a prime, and with fields such as $\mathbb{Q}[\sqrt{2}]$ that contain $\mathbb{Q}$ and are contained in $\mathbb{C}$.

In Book C, you saw the relevance of polynomials over a field to number theory. Polynomials over a field can also represent geometric curves, so another application of fields is that they provide a suitable context to treat certain geometric questions by algebraic methods – this is what is done in a central branch of mathematics called algebraic geometry. Later in this book, in Chapter 20, we will discuss a different and much more recent application of field theory, namely certain methods for coding messages that are essential for secure online information exchange.

We start the chapter by discussing field isomorphisms, and then we look at further constructions of fields. In Chapter 17 we saw that the quotient of a ring by a maximal ideal is in fact a field. A particular case of this construction is obtained by taking the quotient of the polynomial ring $F[x]$ over a field F by a maximal ideal $\langle p(x)\rangle$, where $p(x)$ is an irreducible polynomial. For example, the polynomial $p(x) = x^2 - 2$ in $\mathbb{Q}[x]$ gives rise in this way to a field that is isomorphic to $\mathbb{Q}[\sqrt{2}]$. We find an interesting contrast between the case where $F = \mathbb{Q}$ and where F is a finite field.

We then introduce the *characteristic* of a field, which is the least positive number m such that

$$\underbrace{1+1+1+\cdots+1}_{m \text{ times}} = 0.$$

When this number exists, it must be a prime p, and we then say that the field has characteristic p. When no such number exists, we say that the field has characteristic zero. So, for example, a finite field with p elements has characteristic p, and the fields $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$ have characteristic zero.

Section 2 looks at field extensions. Whenever a field E contains an isomorphic copy of another field F, we say that E is an *extension field* of F. For example, when we quotient a polynomial ring $F[x]$ over a field F by maximal ideal M in $F[x]$, the quotient $F[x]/M$ contains (a copy of) F as a subfield, so $F[x]/M$ is an extension of F. It turns out that any extension of a field F is also a vector space over F. Since vector spaces over arbitrary fields may not be familiar to you, we define them and list their basic properties.

If E is a field extension of F and α is an element of E that is a root of a non-zero polynomial in $F[x]$, then we say that α is *algebraic* over F. Otherwise, we say that α is *transcendental* over F. Familiar examples of elements of $\mathbb{R}$ that are transcendental over $\mathbb{Q}$ are the numbers e and π. We conclude Section 2 with a description of the different properties of

algebraic extensions (those where every element is algebraic over the base field) and transcendental ones.

Section 3 looks at finite fields in some detail. We show that the multiplicative group of such fields is cyclic and we practise calculations in finite fields.

In Section 4 we look at field extensions that contain all the roots of a given polynomial $p(x)$, and introduce the notion of a *splitting field* for $p(x)$, that is, the smallest extension of the field that contains all the roots of $p(x)$. The chapter ends with a classification of finite fields, achieved by showing that for any prime power p^n there is a finite field of order p^n, and then that any two such fields are isomorphic.

Chapter guide

The second section is the most substantial and we expect it to require about twice the study time as the other sections. Sections 1, 3 and 4 have similar contents and we expect them to require similar study times. Many of the exercises involve working modulo p for a prime p.

1 Preliminaries

In this section we introduce two notions that are fundamental to our work on fields, that is, isomorphisms between fields and the characteristic of a field.

1.1 Isomorphisms and homomorphisms between fields

In Definition 1.4 of Chapter 17, we introduced ring homomorphisms. Since fields are a special type of ring, it is natural to ask whether the existence of a ring isomorphism between two fields also preserves the field structure – in other words, whether the isomorphism preserves inverses.

The next proposition shows that this is in fact the case for any ring homomorphism, hence in particular for an isomorphism.

Proposition 1.1

Let F_1 and F_2 be fields and suppose that $\theta : F_1 \to F_2$ is a ring homomorphism. If $a \in F_1$ with $a \neq 0$, then

$$\theta(a^{-1}) = \theta(a)^{-1}.$$

Proof Since θ is a ring homomorphism,

$$\theta(a)\theta(a^{-1}) = \theta(aa^{-1}) = \theta(1_{F_1}) = 1_{F_2}.$$

Thus $\theta(a^{-1}) = \theta(a)^{-1}$ as required. ■

Proposition 1.1 allows us to define two fields to be isomorphic precisely when they are isomorphic as rings.

Definition 1.2 *Isomorphism of fields*

Let F_1 and F_2 be fields. We say that F_1 and F_2 are **isomorphic** if, and only if, there is a ring isomorphism $\theta : F_1 \to F_2$. We then also say that θ is a **field isomorphism**.

We illustrate this definition by working out a particular isomorphism of two infinite fields.

Example 1.3 *A field isomorphism*

In Example 1.7(b) of Chapter 17 we met the field of rational functions $\mathbb{Q}(x)$, which can be constructed as the field of fractions of the polynomial ring $\mathbb{Q}[x]$.

Let $r(x) = \dfrac{s(x)}{t(x)}$ be a rational function over $\mathbb{Q}$, that is, an element of $\mathbb{Q}(x)$ and let $\alpha \in \mathbb{C}$ be such that $t(\alpha) \neq 0$. Denote by $r(\alpha)$ the evaluation of the rational function $r(x)$, that is, the value $\dfrac{s(\alpha)}{t(\alpha)}$.

Now let us define two sets A and B as follows:

$$A = \{r(e) : r(x) \text{ a rational function over } \mathbb{Q}\}, \quad \text{and}$$
$$B = \{r(\pi) : r(x) \text{ a rational function over } \mathbb{Q}\},$$

where e denotes the base of the natural logarithm.

It is known that neither e nor π are roots of a polynomial in $\mathbb{Q}[x]$, so both these sets are well-defined subsets of $\mathbb{R}$. A little more detail on this will be given in Example 2.18. Since rational functions are closed under addition, multiplication, subtraction and (non-zero) division, and since both sets contain 1, it follows that A and B are both subfields of $\mathbb{R}$.

Let $\theta : A \to B$ be defined by

$$\theta : r(e) \mapsto r(\pi),$$

so that, for example, $\theta(1 + e) = 1 + \pi$. Then θ is a field isomorphism. We will show this in Corollary 2.32.

In the next exercise, you are asked to prove a result on ring isomorphisms that we will use repeatedly.

Exercise 1.1

Let F be a field and R be a ring. Suppose that $f\colon F \to R$ is a non-zero ring homomorphism, that is, such that $\mathrm{Im}(f) \neq \{0\}$. Show that $\mathrm{Im}(f)$ is a field isomorphic to F.

Maps where the image of the domain is isomorphic to the domain are known as **embeddings**. Exercise 1.1 proves the following proposition.

Proposition 1.4

Let F and K be fields and suppose that $f\colon F \to K$ is a non-zero ring homomorphism. Then f is an embedding, that is $\mathrm{Im}\, f \cong F$.

We next prove a proposition about quotient fields of polynomial rings that will be repeatedly used in this chapter.

Proposition 1.5

Let F be a field and let $p(x)$ be an irreducible polynomial in $F[x]$. Then $E = F[x]/\langle p(x)\rangle$ is a field.

Proof $F[x]$ is a Euclidean domain (by Example 3.2 of Book C, Chapter 12) and so, by Corollary 2.11 of Chapter 17, $F[x]$ is a PID. Thus, by Theorem 4.22 of Chapter 17, as the polynomial $p(x)$ is irreducible over $F[x]$, the ideal $\langle p(x)\rangle$ is maximal. We can deduce from Theorem 4.23 of Chapter 17 that E is a field. ■

In the next example you will see two particular instances of fields of the form described in Proposition 1.5. As you will see while reading this chapter, this type of construction is a rich source of fields. In fact, in the last section you will learn that all finite fields arise as quotients of this kind.

Example 1.6 *Fields as quotients of polynomial rings*

(a) Let $K = \mathbb{Q}[x]/\langle x^2 - 2\rangle$. Since $x^2 - 2$ is irreducible in $\mathbb{Q}[x]$, K is a field by Proposition 1.5. Let $\theta : \mathbb{Q}[x] \to K$ be the natural homomorphism.

Let $\alpha = \theta(x) = x + \langle x^2 - 2\rangle$. Our aim is to write the elements of K in terms of $\mathbb{Q}$ and α.

For any $f(x) \in \mathbb{Q}[x]$ we use the Division Algorithm to write

$$\begin{aligned} f(x) &= q(x)(x^2 - 2) + r(x) \text{ where } \deg r(x) < 2 \\ &= q(x)(x^2 - 2) + a + bx \text{ for some } a, b \in \mathbb{Q}. \end{aligned}$$

Rearranging terms gives

$$f(x) - (a + bx) = q(x)(x^2 - 2) \in \langle x^2 - 2 \rangle$$

or, equivalently by Proposition 4.2 of Chapter 17,

$$f(x) + \langle x^2 - 2 \rangle = a + bx + \langle x^2 - 2 \rangle = a + b\alpha.$$

Hence every element $f(x) + \langle x^2 - 2 \rangle$ of K can be written uniquely as $a + b\alpha$ with $a, b \in \mathbb{Q}$. Consequently, we can regard K as a field whose underlying set is $\{a + b\alpha : a, b \in \mathbb{Q}\}$, and where addition and multiplication are defined as follows.

$$\begin{aligned}(a + b\alpha) + (c + d\alpha) &= (a + c) + (b + d)\alpha \\ (a + b\alpha)(c + d\alpha) &= ac + bd\alpha^2 + (ad + bc)\alpha \\ &= ac + 2bd + (ad + bc)\alpha\end{aligned}$$

(since $\alpha^2 = x^2 + \langle x^2 - 2 \rangle = 2 + x^2 - 2 + \langle x^2 - 2 \rangle = 2 + \langle x^2 - 2 \rangle$)

Note that addition and multiplication of constant polynomials correspond to addition and multiplication in $\mathbb{Q}$, so that there is a one–one homomorphism from $\mathbb{Q}$ to K.

In Book C, Chapter 11, Exercise 1.10, the field $\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$ was introduced as a subfield of $\mathbb{R}$. Since in $\mathbb{Q}[\sqrt{2}]$ we have

$$(a + b\sqrt{2})(c + d\sqrt{2}) = ac + 2bd + (ad + bc)\sqrt{2},$$

it follows from the preceding calculations that the map $\psi : K \to \mathbb{Q}[\sqrt{2}]$ defined by

$$\psi : a + b\alpha \mapsto a + b\sqrt{2}$$

is an isomorphism.

(b) Let $L = \mathbb{Z}_7[x]/\langle x^2 - 3 \rangle$. Since 3 is a quadratic non-residue over 7, $x^2 - 3$ is irreducible over $\mathbb{Z}_7[x]$ and, by Proposition 1.5, L is a field. Let $\theta : \mathbb{Z}_7[x] \to L$ be the natural homomorphism.

Let $\alpha = \theta(x) = x + \langle x^2 - 3 \rangle$. As in part (a) we aim to show that the elements of L can be written in terms of $\mathbb{Z}_7$ and α.

If $f(x) \in \mathbb{Z}_7[x]$, we use the Division Algorithm to write

$$\begin{aligned}f(x) &= q(x)(x^2 - 3) + r(x) \text{ where } \deg r(x) < 2 \\ &= q(x)(x^2 - 3) + a + bx \text{ for some } a, b \in \mathbb{Z}_7.\end{aligned}$$

Thus, we have

$$f(x) - (a + bx) = q(x)(x^2 - 3) \in \langle x^2 - 3 \rangle,$$

which gives

$$f(x) + \langle x^2 - 3 \rangle = a + bx + \langle x^2 - 3 \rangle = a + b\alpha.$$

It follows that every element of L can be written uniquely as $a + bx + \langle x^2 - 3\rangle = a + b\alpha$, where $a, b \in \mathbb{Z}_7$. Hence we can regard L as a field with underlying set $\{a + b\alpha : a, b \in \mathbb{Z}_7\}$ and with addition and multiplication defined by

$$\begin{aligned}(a + b\alpha) + (c + d\alpha) &= (a + c) + (b + d)\alpha \pmod 7\\ (a + b\alpha)(c + d\alpha) &= ac + bd\alpha^2 + (ad + bc)\alpha\\ &= ac + 3bd + (ad + bc)\alpha \pmod 7\end{aligned}$$

since $\alpha^2 = x^2 + \langle x^2 - 3\rangle = 3 + (x^2 - 3) + \langle x^2 - 3\rangle = 3 + \langle x^2 - 3\rangle$.

The next proposition generalises Examples 1.6(a) and (b) to any field F and irreducible polynomial in $F[x]$. In the proof, division in the ring $F[x]$ can be carried out using the Division Algorithm given in Book C, Chapter 11, Theorem 3.1.

Proposition 1.7

Let $p(x) = p_0 + p_1x + \cdots + p_nx^n$ be an irreducible polynomial over a field F, so that $E = F[x]/\langle p(x)\rangle$ is a field. Let $\theta : F[x] \to E$ be the natural homomorphism and let $\alpha = \theta(x) = x + \langle p(x)\rangle$. Then:

(a) Any element of E can be represented, uniquely, in the form

$$a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1},$$

where $a_0, a_1, \ldots, a_{n-1} \in F$.

With this representation of elements of E, addition is given by

$$\begin{aligned}&(a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1}) + (b_0 + b_1\alpha + \cdots + b_{n-1}\alpha^{n-1})\\ &\qquad = a_0 + b_0 + (a_1 + b_1)\alpha + \cdots + (a_{n-1} + b_{n-1})\alpha^{n-1},\end{aligned}$$

and multiplication is given by

$$\begin{aligned}&(a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1})(b_0 + b_1\alpha + \cdots + b_{n-1}\alpha^{n-1})\\ &\qquad = (r_0 + r_1\alpha + \cdots + r_{n-1}\alpha^{n-1}),\end{aligned}$$

where $r_0 + r_1x + \cdots + r_{n-1}x^{n-1} \in F[x]$ is the remainder in the division of $(a_0 + a_1x + \cdots + a_{n-1}x^{n-1})(b_0 + b_1x + \cdots + b_{n-1}x^{n-1})$ by $p(x)$.

(b) In E, we have

$$p(\alpha) = p_0 + p_1\alpha + \cdots + p_n\alpha^n = 0,$$

which means that α can be regarded as a root of the polynomial $p(x)$ with this representation of the elements of E.

Proof Since $p(x)$ is irreducible over $F[x]$, E is a field by Proposition 1.5.

(a) Firstly, $p(x)$ is irreducible, and so it has degree at least one. Thus, for $a \in F$ we have $\theta(a) = a + \langle p(x) \rangle$, so that

$$\theta(ax^m) = \theta(a)\theta(x)^m = a\alpha^m.$$

Hence if $f(x) = a_0 + a_1 x + \cdots + a_m x^m$ with $a_0, a_1, \ldots, a_m \in F$, then

$$\theta(f(x)) = a_0 + a_1\alpha + \cdots + a_m\alpha^m = f(\alpha).$$

Let $f(x)$ be a polynomial in $F[x]$. We use the Division Algorithm to write

$$f(x) = q(x)p(x) + r(x)$$

where $\deg r(x) < \deg p(x)$, or, equivalently,

$$f(x) = q(x)p(x) + r_0 + r_1 x + \cdots + r_{n-1}x^{n-1}$$

Some of the r_i could be 0.

for some $r_0, r_1, \ldots, r_{n-1} \in F$.

Proceeding as in Example 1.6 gives

$$f(x) - (r_0 + r_1 x + \cdots + r_{n-1}x^{n-1}) = q(x)p(x) \in \langle p(x) \rangle,$$

which can be written in the form

$$\begin{aligned} f(x) + \langle p(x) \rangle &= r_0 + r_1 x + \cdots + r_{n-1}x^{n-1} + \langle p(x) \rangle \\ &= r_0 + r_1\alpha + \cdots + r_{n-1}\alpha^{n-1}. \end{aligned}$$

Thus every element of E can be represented uniquely in the form

$$r_0 + r_1\alpha + \cdots + r_{n-1}\alpha^{n-1},$$

where $r_0, r_1, \ldots, r_{n-1} \in F$.

We can therefore regard E as a field with underlying set

$$\{a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} : a_0, a_1, \ldots, a_{n-1} \in F\}.$$

The homomorphism properties of θ ensure that the definition of addition and multiplication are correct when the elements of E are represented in this way.

(b) Since $\theta(p(x)) = 0$, we have
$p(\alpha) = p_0 + p_1\alpha + \cdots + p_n\alpha^n = \theta(p(x)) = 0.$ ■

The idea that the product of two elements is a remainder on division is one that you have already met when working in $\mathbb{Z}_n$. Just as we say in that case that multiplication is 'modulo n' and write $\pmod n$ in calculations to make this clear, we will describe multiplication in the quotient $F[x]/\langle p(x) \rangle$ as 'modulo $p(\alpha)$', and write $\pmod{p(\alpha)}$ where appropriate.

The next exercise illustrates Proposition 1.7.

Exercise 1.2

Let $p(x) = x^2 - x + 1$ be a polynomial in $\mathbb{Q}[x]$.

(a) Show that $p(x)$ is irreducible over $\mathbb{Q}[x]$.

(b) Let $E = \mathbb{Q}[x]/\langle p(x)\rangle$. Let $\alpha = x + \langle p(x)\rangle$ so that the elements of E can be written in the form $a + b\alpha$ where $a, b \in \mathbb{Q}$ as in Proposition 1.7. Write down the rule for multiplying two elements represented in this way.

In Example 1.6(a), we observed that the field $\mathbb{Q}[x]/\langle x^2 - 2\rangle$ is isomorphic to $\mathbb{Q}[\sqrt{2}]$. Similarly, $\mathbb{Q}[x]/\langle x^2 + 1\rangle \cong \mathbb{Q}[i]$; in fact, you saw this example just before Theorem 4.23 of Chapter 17. These isomorphisms enable us to carry out calculations using the more convenient notation $a + b\sqrt{2}$ and $a + bi$, respectively. The next worked exercise uses this approach when working over a finite field, as the mild abuse of notation improves readability.

Worked Exercise 1.8

(a) Show that $\mathbb{Z}_{13}[x]/\langle x^2 - 2\rangle$ and $\mathbb{Z}_{13}[x]/\langle x^2 - 5\rangle$ are fields.

(b) Show that the fields $\mathbb{Z}_{13}[x]/\langle x^2 - 2\rangle$ and $\mathbb{Z}_{13}[x]/\langle x^2 - 5\rangle$ are isomorphic.

Solution

(a) From the solution to Book C, Chapter 10, Exercise 1.2 we know that neither 2 nor 5 have square roots modulo 13, that is 2 and 5 are both quadratic non-residues of 13. Hence the two polynomials are irreducible and so $\mathbb{Z}_{13}[x]/\langle x^2 - 2\rangle$ and $\mathbb{Z}_{13}[x]/\langle x^2 - 5\rangle$ are fields by Proposition 1.5.

(b) By Proposition 1.7, the elements of $\mathbb{Z}_{13}[x]/\langle x^2 - 2\rangle$ can be written as $a + b\alpha$ where $a, b \in \mathbb{Z}_{13}$, with $\alpha^2 = 2$, and those of $\mathbb{Z}_{13}[x]/\langle x^2 - 5\rangle$ can be written as $c + d\beta$ with $\beta^2 = 5$ where $c, d \in \mathbb{Z}_{13}$.

To improve readability, we will mildly abuse notation by writing $\sqrt{2}$ for α and $\sqrt{5}$ for β.

We wish to define an isomorphism $\psi : \mathbb{Z}_{13}[x]/\langle x^2 - 2\rangle \to \mathbb{Z}_{13}[x]/\langle x^2 - 5\rangle$. In order to do this, we need to suitably define the image $\psi(a + b\sqrt{2})$ of an element of $\mathbb{Z}_{13}[x]/\langle x^2 - 2\rangle$.

Simply defining $\psi(a + b\sqrt{2}) = a + b\sqrt{5}$ will not work, since then

$$\psi(2) = \psi(\sqrt{2})\psi(\sqrt{2}) = \sqrt{5}\sqrt{5} = 5 \not\equiv 2 \pmod{13}.$$

So we need to define $\psi(\sqrt{2}) = r + s\sqrt{5}$ where $(r + s\sqrt{5})^2 \equiv 2 \pmod{13}$. In other words, we require r and s such that

$$(r + s\sqrt{5})^2 = r^2 + 5s^2 + 2rs\sqrt{5} \equiv 2 \pmod{13}.$$

This means that either r or s is zero. Since we know that 2 is a quadratic non-residue of 13, we have $r = 0$. Thus we require s such that $5s^2 \equiv 2 \pmod{13}$, that is so that $s^2 \equiv 3 \pmod{13}$. Since 3 is a quadratic residue of 13, and $4^2 \equiv 3 \pmod{13}$, we can choose $s = 4$.

Let $\psi(a + b\sqrt{2}) = a + 4b\sqrt{5}$ so that $\psi^{-1}(c + d\sqrt{5}) = c + 10d\sqrt{2}$ (as $4 \times 10 \equiv 1 \pmod{13}$). Therefore ψ is a bijection, and since $\psi(1) = 1$ we only have to show the isomorphism properties for addition and multiplication. For addition we have

$$\begin{aligned}\psi(a + b\sqrt{2}) + \psi(c + d\sqrt{2}) &= a + 4b\sqrt{5} + c + 4d\sqrt{5} \\ &= (a + c) + 4(b + d)\sqrt{5} \\ &= \psi(a + c + (b + d)\sqrt{2}) \\ &\equiv \psi((a + b\sqrt{2}) + (c + d\sqrt{2})) \pmod{13}.\end{aligned}$$

For multiplication we have

$$\begin{aligned}\psi(a + b\sqrt{2})\psi(c + d\sqrt{2}) &= (a + 4b\sqrt{5})(c + 4d\sqrt{5}) \\ &\equiv ac + 2bd + 4(ad + bc)\sqrt{5} \pmod{13}\end{aligned}$$

since $80 \equiv 2 \pmod{13}$, and

$$\begin{aligned}\psi((a + b\sqrt{2})(c + d\sqrt{2})) &= \psi(ac + 2bd + (ad + bc)\sqrt{2}) \\ &\equiv ac + 2bd + 4(ad + bc)\sqrt{5} \pmod{13}.\end{aligned}$$

Hence ψ is a field homomorphism.

Exercise 1.3

(a) Show that $\mathbb{Z}_7[x]/\langle x^2 - 5\rangle$ and $\mathbb{Z}_7[x]/\langle x^2 - 6\rangle$ are fields.

(b) Show that the fields $\mathbb{Z}_7[x]/\langle x^2 - 5\rangle$ and $\mathbb{Z}_7[x]/\langle x^2 - 6\rangle$ are isomorphic.

This subsection concludes with an exercise targeting the fields of rational and complex numbers.

Exercise 1.4

(a) Show that $\mathbb{Q}[x]/\langle x - 2\rangle \cong \mathbb{Q}$.

(b) Let $p(x)$ be an irreducible polynomial over $\mathbb{C}[x]$. Show that $\mathbb{C}[x]/\langle p(x)\rangle \cong \mathbb{C}$.

1.2 Characteristic of a field

The fields you have met so far either contain $\mathbb{Q}$ or $\mathbb{Z}_p$, where p is a prime, or they are obtained from $\mathbb{Q}$ or $\mathbb{Z}_p$ by a construction such as in Proposition 1.5. We will now show that this is always the case. We start by defining the *characteristic* of a field.

Definition 1.9 *Characteristic of a field*

If the order of 1 in the additive group $(F, +)$ of a field F is infinite, then F is said to have **characteristic zero**. If the order of 1 in the group $(F, +)$ is finite and equal to m, we say that the field F has **characteristic** m.

Next we prove that the possibilities for the non-zero characteristic of a field are rather restricted.

Theorem 1.10

The characteristic of any field is either prime or zero.

Proof Assume that F is a field of some positive characteristic m. That is, in F we have $0 = 1 + 1 + \cdots + 1$ where the sum contains exactly m terms, and m is the smallest positive integer for which this equality holds.

Suppose that m is not a prime and let $m = m_1 m_2$ where m_1 and m_2 are positive integers smaller than m. Then, in F we would have

$$0 = (\underbrace{1 + 1 + \cdots + 1}_{m_1 \text{ times}})(\underbrace{1 + 1 + \cdots + 1}_{m_2 \text{ times}}).$$

However, this gives two non-zero elements of F whose product is zero, which contradicts the fact that a field cannot contain zero divisors.

Therefore if the characteristic of F is finite, it must be prime. Summing up, the characteristic of any field is zero or prime. ■

A key fact that you should be aware of is that in a field of characteristic p, any multiple of $p \cdot 1$, that is, any multiple of $1 + \cdots + 1$ where the sum has p terms, is zero.

The next exercise asks you to identify a particular subfield of a field of prime characteristic.

Exercise 1.5

Let F be a field of prime characteristic p. Consider the subset

$$K = \{0,\ 1,\ 1+1,\ \ldots,\ \underbrace{1+1+\cdots+1}_{p-1 \text{ times}}\} \subset F$$

that contains all possible sums of the multiplicative identity 1. Show that K is a subfield of F.

Motivated by Exercise 1.5, we now state and prove a theorem about the smallest subfields of fields of prime and zero characteristic.

Theorem 1.11

If a field F has prime characteristic p, then F contains a subfield isomorphic to $\mathbb{Z}_p$, and this is the smallest subfield of F with respect to inclusion, that is, it is contained in every other subfield of F.

Similarly, if F has characteristic zero, then F contains a subfield isomorphic to $\mathbb{Q}$, and this is the smallest subfield of F with respect to inclusion.

Proof Let F have prime characteristic p. Consider the elements 0, 1, $1+1$, $\ldots$, up to $1+1+\cdots+1$ where the sum has $p-1$ terms. We know from the solution to Exercise 1.5 that the set formed by these p elements forms a subfield K of F and that the mapping $\theta : \mathbb{Z}_p \to K$ that maps the residue class $0 \pmod p$ onto the element $0 \in K$ and, for $1 \leq k \leq p-1$, the residue class $k \pmod p$ onto the sum $1+1+\cdots+1 \in K$ with k terms is a homomorphism. Hence, by the solution to Exercise 1.1, θ is an isomorphism of fields since $K = \mathrm{Im}(\theta)$.

To prove minimality, observe that any subfield of F must contain the multiplicative identity 1. But since, as we have seen above, this multiplicative unit generates the subfield K that is isomorphic to $\mathbb{Z}_p$, we conclude that K is the smallest subfield of F, that is, it is contained in any other subfield of F.

Let F have characteristic 0 and consider the elements $1+1$, $1+1+1$, and so on, together with their additive inverses. By an argument similar to that above, F must contain an isomorphic copy of the integers. Since F is a field, it must also contain multiplicative inverses to all the non-zero elements that are in this isomorphic copy. That is, F must contain an isomorphic copy of all integers m and all reciprocals $\frac{1}{n}$ of non-zero elements n. But again, since F is a field, it must contain the product of any two of its elements, and hence it must contain all fractions $m \cdot \frac{1}{n} = \frac{m}{n}$. We conclude that F contains an isomorphic copy of $\mathbb{Q}$. ■

The smallest subfield of a field F of prime or zero characteristic, referred to in Theorem 1.11, is often called the **prime field** of F.

Theorem 1.11 also shows that, up to isomorphism, there is only one field of p elements for any given prime p. Until now we have used the notation $\mathbb{Z}_p$ for this field and we will continue to do so. There is, however, an alternative notation, namely, GF_p, read as the **Galois field of p elements**. This notation honours Evariste Galois, who was a major influence on the development of the theory of finite fields.

The next result is often useful when working in a field of characteristic p. It is sometimes known as the **Idiot's Binomial Theorem**.

Theorem 1.12

Let F be a field of characteristic p. Then

$$(u+v)^p = u^p + v^p$$

for all $u, v \in F$.

Remember that $\binom{p}{j} = \dfrac{p!}{(p-j)!j!}$.

Proof Using the binomial theorem to expand $(u+v)^p$ yields

$$(u+v)^p = u^p + \binom{p}{1}u^{p-1}v + \cdots + \binom{p}{j}u^{p-j}v^j + \cdots + \binom{p}{p-1}uv^{p-1} + v^p \ .$$

However, here every binomial coefficient $\binom{p}{j}$ is to be interpreted as the sum $1+1+\cdots+1$ with $\binom{p}{j}$ terms. Now, for each j such that $1 \leq j \leq p-1$, we have $p \mid p!$, $p \nmid (p-j)!$ and $p \nmid j!$, and so $\binom{p}{j}$ is a multiple of p. Thus $\binom{p}{j} = 0$ in the field F. Hence in the field F the above binomial expansion reduces to $(u+v)^p = u^p + v^p$. ■

A word of caution regarding prime characteristic: you should not think that a field of prime characteristic is necessarily finite. For an example of an infinite field of finite characteristic, you are invited to consider the field of fractions of the ring $\mathbb{Z}_p[x]$ for an arbitrary prime p.

This section ends with two results relating field isomorphisms and characteristic. The first result proves that isomorphic fields have the same characteristic.

Proposition 1.13

Let F_1 and F_2 be fields and suppose that there is a non-zero field homomorphism $\phi : F_1 \to F_2$. Then F_1 and F_2 have the same characteristic.

Proof Suppose that F_1 has characteristic 0. Then, by Theorem 1.11, F_1 has a subfield isomorphic to $\mathbb{Q}$. Since, by Proposition 1.4, F_2 has a subfield isomorphic to F_1, it also has a subfield isomorphic to $\mathbb{Q}$. Thus 1 has infinite order in F_2 and F_2 has characteristic 0.

Suppose that F_1 has finite characteristic p for some prime p. Theorem 1.11 then tells us that F_1 has a subfield isomorphic to $\mathbb{Z}_p$. As above, since F_2

has a subfield isomorphic to F_1, it also has a subfield isomorphic to $\mathbb{Z}_p$. Thus 1 has finite order p in F_2 and F_2 has characteristic p. ■

The final result of this section tells us that any isomorphism between subfields of $\mathbb{C}$ is the identity map on $\mathbb{Q}$.

Theorem 1.14

Let F_1 and F_2 be subfields of $\mathbb{C}$ and let $\phi : F_1 \to F_2$ be an embedding. Then $\phi(x) = x$ for every $x \in \mathbb{Q}$.

Proof By Theorem 1.11, $\mathbb{Q}$ is a subfield of both F_1 and F_2. Since ϕ must preserve the additive and the multiplicative identities, we have $\phi(0) = 0$ and $\phi(1) = 1$. By the definition of a field homomorphism, for any positive integer m we have

$$\phi(m) = \phi(\underbrace{1 + \cdots + 1}_{m \text{ times}}) = \underbrace{\phi(1) + \cdots + \phi(1)}_{m \text{ times}} = m.$$

This means that $\phi(m) = m$ for every positive integer m. As ϕ preserves additive inverses, $\phi(-m) = -m$ and hence $\phi(n) = n$ for all integers n. Since ϕ also preserves multiplicative inverses, for each non-zero integer n we have

$$\phi\left(\frac{1}{n}\right) = \frac{1}{\phi(n)} = \frac{1}{n}.$$

Finally, from the properties of a field homomorphism we deduce that for all integers m, n with $n \neq 0$ we have

$$\phi\left(\frac{m}{n}\right) = \phi\left(m \cdot \frac{1}{n}\right) = \phi(m) \cdot \phi\left(\frac{1}{n}\right) = \frac{m}{n}.$$

This shows that $\phi(x) = x$ for all $x \in \mathbb{Q}$. ■

2 Field extensions

This section introduces field extensions. We start with the definition of a field extension and then look at some examples. We will see how regarding an extension of a field F as a vector space over F allows us to determine some key properties of extensions – in particular their *degree*, which is, in a sense that will be made clear, a measure of dimension. We then go on to study some particular types of extension.

Definition 2.1 *Extension of a field*

A field E is an **extension of a field** F if F is a subfield of E.

In the next two examples we will use the word 'identify'. We used it before when regarding integers as a subset of $\mathbb{Q}$ in Chapter 17, and also when regarding a ring R as a subring of the ring of polynomials $R[x]$ by 'identifying' the constant polynomials with R. When we say that we *identify* two isomorphic objects, such as two fields, we mean that we regard them as not just isomorphic, but equal. The main place where we use this idea is in connection with the natural homomorphism from a polynomial ring over a field F to a quotient ring over a maximal ideal M; in this setting, we identify F with its image $\{k + M : k \in F\}$ under the natural homomorphism.

Example 2.2 *Some field extensions*

(a) $\mathbb{C}$ is an extension of $\mathbb{Q}$.

(b) Let $E = \{a + b\alpha : a, b \in \mathbb{Q}\}$, where $\alpha^2 = 2$. Define addition and multiplication on E by

$$(a + b\alpha) + (c + d\alpha) = (a + c) + (b + d)\alpha,$$
$$(a + b\alpha)(c + d\alpha) = ac + 2bd + (ad + bc)\alpha.$$

Then, as you saw in Example 1.6(a), E is a field isomorphic to $\mathbb{Q}[x]/\langle x^2 - 2\rangle$. The subset $F = \{a + b\alpha : a \in \mathbb{Q}, b = 0\}$ of E is isomorphic to $\mathbb{Q}$ and E is an extension of F. In this type of example we usually identify $\mathbb{Q}$ with F (as we do when regarding the integers as a subset of $\mathbb{Q}$) and say that E is an extension of $\mathbb{Q}$.

(c) Let $E = \{a + b\alpha : a, b \in \mathbb{Z}_7\}$, where $\alpha^2 = 3$. Define addition and multiplication on E by

$$(a + b\alpha) + (c + d\alpha) = (a + c) + (b + d)\alpha \pmod 7,$$
$$(a + b\alpha)(c + d\alpha) = ac + 3bd + (ad + bc)\alpha \pmod 7.$$

Again, by Example 1.6(b), E is a field isomorphic to $\mathbb{Z}_7[x]/\langle x^2 - 3\rangle$. The subset $F = \{a + b\alpha : a \in \mathbb{Z}_7, b = 0\}$ of E is isomorphic to $\mathbb{Z}_7$ and E is an extension of F. As in the previous example, we identify $\mathbb{Z}_7$ with F and say that E is an extension of $\mathbb{Z}_7$.

2.1 Vector spaces

One way to look at field extensions is to think in terms of vector spaces. In order to do this we need to consider vector spaces where the scalars come from a general field. In your previous studies you have met vector spaces where the scalars are real numbers. However, the definition of a vector space over $\mathbb{R}$ and the key notions only make use of the field properties of $\mathbb{R}$, and so they are easily extended to the case where the scalars come from an arbitrary field.

Definition 2.3 *Vector spaces over general fields*

A **vector space over a field** F consists of a set V of elements and two operations – vector addition and scalar multiplication – such that the following axioms hold.

Axioms for vector addition:

A1 Closure of vector addition For all $\mathbf{v}_1, \mathbf{v}_2 \in V$,

$$\mathbf{v}_1 + \mathbf{v}_2 \in V.$$

A2 Additive identity There is a vector $\mathbf{0} \in V$ such that for each $\mathbf{v} \in V$,

$$\mathbf{v} + \mathbf{0} = \mathbf{0} + \mathbf{v} = \mathbf{v}.$$

A3 Inverses For each $\mathbf{v} \in V$, there is an element $-\mathbf{v}$ (its additive inverse) such that

$$\mathbf{v} + (-\mathbf{v}) = (-\mathbf{v}) + \mathbf{v} = \mathbf{0}.$$

A4 Associativity of vector addition For all $\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3 \in V$,

$$(\mathbf{v}_1 + \mathbf{v}_2) + \mathbf{v}_3 = \mathbf{v}_1 + (\mathbf{v}_2 + \mathbf{v}_3).$$

A5 Commutativity For all $\mathbf{v}_1, \mathbf{v}_2 \in V$,

$$\mathbf{v}_1 + \mathbf{v}_2 = \mathbf{v}_2 + \mathbf{v}_1.$$

Axioms for scalar multiplication:

S1 Closure under scalar multiplication For all $\mathbf{v} \in V$ and $\alpha \in F$,

$$\alpha\mathbf{v} \in V.$$

S2 Associativity of scalar multiplication For all $\mathbf{v} \in V$ and $\alpha, \beta \in F$,

$$\alpha(\beta\mathbf{v}) = (\alpha\beta)\mathbf{v}.$$

S3 Scalar identity For all $\mathbf{v} \in V$,

$$1\mathbf{v} = \mathbf{v}.$$

Axioms combining addition and multiplication:

D1 Distributive law For all $\mathbf{v}_1, \mathbf{v}_2 \in V$ and $\alpha \in F$,

$$\alpha(\mathbf{v}_1 + \mathbf{v}_2) = \alpha\mathbf{v}_1 + \alpha\mathbf{v}_2.$$

D2 Distributive law For all $\mathbf{v} \in V$ and $\alpha, \beta \in F$,

$$(\alpha + \beta)\mathbf{v} = \alpha\mathbf{v} + \beta\mathbf{v}.$$

Observe that axioms A1–A5 say that $(V, +)$ is an abelian group.

With Definition 2.3 in mind, we revisit Example 2.2 to see how we can view an extension of a field as a vector space over that field.

Example 2.4

(a) Consider the field of complex numbers $\mathbb{C} = \{a + ib : a, b \in \mathbb{R}\}$. We can regard $\mathbb{C}$ as a vector space over $\mathbb{R}$. We can also regard it as a vector space over $\mathbb{Q}$ where scalar multiplication is just multiplication of a complex number by a rational number.

(b) Let us revisit the field $E = \{a + b\alpha : a, b \in \mathbb{Q}\}$ in Example 2.2(b), where $\alpha^2 = 2$ and addition and multiplication on E are given by

$$(a + b\alpha) + (c + d\alpha) = (a + c) + (b + d)\alpha,$$
$$(a + b\alpha)(c + d\alpha) = ac + 2bd + (ad + bc)\alpha.$$

We can also view E as a vector space over $\mathbb{Q}$. Since E is a field, $(E, +)$ is an abelian group, and so axioms A1–A5 are satisfied. Scalar multiplication is defined using the definition of multiplication above with $b = 0$, so that for $a \in \mathbb{Q}$ and $c + d\alpha \in E$,

$$a(c + d\alpha) = ac + ad\alpha.$$

Then axioms S1–S3 and D1–D2 are satisfied because E is a field.

(c) Let us look at the field $E = \{a + b\alpha : a, b \in \mathbb{Z}_7\}$ in Example 2.2(c), where $\alpha^2 = 3$ and addition and multiplication on E are given by

$$(a + b\alpha) + (c + d\alpha) = (a + c) + (b + d)\alpha \pmod 7,$$
$$(a + b\alpha)(c + d\alpha) = ac + 3bd + (ad + bc)\alpha \pmod 7.$$

We can also view E as a vector space over $\mathbb{Z}_7$. Since E is a field, axioms A1–A5 are satisfied. Scalar multiplication is defined using the definition of multiplication above with $b = 0$, so that, again since E is a field, axioms S1–S3 and D1–D2 are satisfied.

The previous examples generalise in a way you might have expected.

Proposition 2.5 *Field extensions as vector spaces*

If E is an extension of a field F, then E is a vector space over F.

Proof Since E is a field, $(E, +)$ is an abelian group, so the (abelian group) axioms A1–A5 are satisfied. Scalar multiplication is defined using the definition of multiplication in F, that is, for $m \in F$ and $v \in E$, the multiple of the vector v by the scalar m is defined to be the product mv in E. Then, since E is a field, axioms S1–S3 and D1–D2 are satisfied. ■

You might object that when we think of a field extension as a vector space we 'hide' some information. But one of the skills needed in mathematics is the ability to view a mathematical object in different ways, and by ignoring some details it is possible to understand other details more clearly.

In our current context we will use the vector space 'view' to introduce the idea of *degree* of a field extension. We first need to recall the relevant notions in a vector space.

Definition 2.6 *Linear independence and basis*

Let V be a vector space over a field F.

(a) Let $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_k \in V$. A **linear combination** of the vectors $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_k$ is a vector of the form

$$\alpha_1\mathbf{v}_1 + \alpha_2\mathbf{v}_2 + \cdots + \alpha_k\mathbf{v}_k,$$

where $\alpha_1, \alpha_2, \ldots, \alpha_k \in F$.

(b) Let $S = \{\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_k\}$ be a finite set of vectors in a vector space V. Then the **span** $\langle S \rangle$ of S is the set of all possible linear combinations

$$\alpha_1\mathbf{v}_1 + \alpha_2\mathbf{v}_2 + \cdots + \alpha_k\mathbf{v}_k,$$

where $\alpha_1, \alpha_2, \ldots, \alpha_k \in F$; that is,

$$\langle S \rangle = \{\alpha_1\mathbf{v}_1 + \alpha_2\mathbf{v}_2 + \cdots + \alpha_k\mathbf{v}_k : \alpha_1, \alpha_2, \ldots, \alpha_k \in F\}.$$

We say that the set of vectors $\{\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_k\}$ **spans** $\langle S \rangle$ or is a **spanning set** for $\langle S \rangle$, and that $\langle S \rangle$ is the set **spanned** by S.

(c) A finite set of vectors $\{\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_k\}$ in a vector space V is a **linearly dependent** set if there exist $\alpha_1, \alpha_2, \ldots, \alpha_k \in F$, *not all zero*, such that

$$\alpha_1\mathbf{v}_1 + \alpha_2\mathbf{v}_2 + \cdots + \alpha_k\mathbf{v}_k = \mathbf{0}.$$

(d) A finite set of vectors $\{\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_k\}$ is **linearly independent** if it is not linearly dependent; that is, if

$$\alpha_1\mathbf{v}_1 + \alpha_2\mathbf{v}_2 + \cdots + \alpha_k\mathbf{v}_k = \mathbf{0}$$

only when $\alpha_1 = \alpha_2 = \cdots = \alpha_k = 0$.

(e) A *basis* for a vector space V is a linearly independent set of vectors that is a spanning set for V.

(f) Let V be a vector space. Then V has **finite dimension** if it contains a finite set of vectors S that forms a basis for V. If no such set exists, then V has **infinite dimension**.

You are now invited to test your understanding of Definition 2.6 on a field you have encountered before.

Exercise 2.1

Consider again the field $E = \{a + b\alpha : a, b \in \mathbb{Q}\}$ in Example 2.2(b), with $\alpha^2 = 2$ and with addition and multiplication defined by

$$(a + b\alpha) + (c + d\alpha) = (a + c) + (b + d)\alpha,$$
$$(a + b\alpha)(c + d\alpha) = ac + 2bd + (ad + bc)\alpha,$$

viewed as an extension of the field $F = \{a + b\alpha : a, b \in \mathbb{Q},\ b = 0\} \cong \mathbb{Q}$. Write down a basis for E, regarded as a vector space over F.

Not all vector spaces have finite dimension. For example, $\mathbb{C}$ as a vector space over $\mathbb{Q}$ does not have a finite basis, and so it has infinite dimension. When a vector space does have a finite basis, the following Basis Theorem (which you may have encountered in your previous studies for vector spaces over $\mathbb{R}$, and the proof of which we omit) tells us that every basis has the same number of elements.

Theorem 2.7 *Basis Theorem*

Let V be a finite-dimensional vector space. Then every basis for V contains the same number of vectors.

This enables us to define the degree of a field extension.

Definition 2.8 *Degree of a field extension*

Let E be an extension of a field F. If E has a finite basis as a vector space over F, we say that the **degree** of the extension is its dimension as a vector space over F, that is, the number of vectors in any basis for the space. We denote the degree by $[E : F]$. If E does not have a finite basis as a vector space over F, then we say that the extension is infinite and we write $[E : F] = \infty$.

Viewing field extensions as vector spaces enables us to show in an elegant way that the order of a finite field is a prime power.

Theorem 2.9

The order of a finite field is a power of a prime.

Proof Let F be a finite field. By the previous results we know that F has characteristic p for some prime p, and it contains (an isomorphic copy of) $\mathbb{Z}_p$ as a subfield.

Now, by Proposition 2.5, the field F is a vector space over the field $\mathbb{Z}_p$. Since F is finite, it has, as a vector space over $\mathbb{Z}_p$, a finite dimension, say, n. Hence, there exists a basis B for the vector space F over $\mathbb{Z}_p$ such that $|B| = n$, say $B = \{\beta_1, \beta_2, \ldots, \beta_n\} \subset F$.

Since B is a basis for F, for every element $\alpha \in F$ there exists a *unique* n-tuple $(c_1, c_2, \ldots, c_n)$ of elements of $\mathbb{Z}_p$ such that

$$\alpha = c_1\beta_1 + c_2\beta_2 + \cdots + c_n\beta_n.$$

Conversely, every linear combination of elements of B with coefficients from $\mathbb{Z}_p$ is an element of F.

This means that the mapping $\alpha \mapsto (c_1, c_2, \ldots, c_n)$ is a bijection from F into the set $(\mathbb{Z}_p)^n$ of all n-tuples of elements of $\mathbb{Z}_p$.

Therefore, $|F| = |(\mathbb{Z}_p)^n| = p^n$. In other words, since this bijection enables us to identify each element of F with an n-tuple of elements of $\mathbb{Z}_p$, and since there are p^n distinct n-tuples of elements of $\mathbb{Z}_p$, we conclude that F must have p^n elements. ■

2.2 Extensions of fields by elements

If E is an extension of a field F and if α is an element of E that may or may not be in F, it makes sense to study the subfields of E that contain F and the element α. Such a point of view leads to a rich theory.

Definition 2.10 $F(\alpha)$

Let E be an extension of a field F and let $\alpha \in E$. We denote by $F(\alpha)$ the smallest subfield of E (with respect to inclusion) that contains both F and α.

A consequence of Definition 2.10 is that $F(\alpha)$ contains, at the very least, the set of all polynomials $a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_r\alpha^r$ for all $r \geq 0$, where $a_i \in F$ for all i such that $0 \leq i \leq r$.

Note the use of round brackets in the notation $F(\alpha)$. Until now we have been using square brackets to denote an extension of a ring, for example $\mathbb{Z}[\sqrt{2}]$ or $\mathbb{Q}[\sqrt{2}]$. In the latter case, the ring is in fact a field (see Example 2.2(a)). In cases like this we will use the round bracket notation from now on.

An extension $F(\alpha)$ is of one of two kinds, determined by whether α is a root of a polynomial in $F[x]$.

Definition 2.11 *Algebraic and transcendental element*

Let the field E be an extension of a field F. An element $\alpha \in E$ is said to be **algebraic over** F if there is a non-zero polynomial $h(x)$ in $F[x]$ with $h(\alpha) = 0$. An element $\alpha \in E$ is called **transcendental over** F if there is no polynomial $h(x)$ in $F[x]$ with $h(\alpha) = 0$.

We also want to consider extensions by several elements. We might, for example, want to extend $\mathbb{Q}$ by both $\sqrt{2}$ and $\sqrt{3}$ if we wanted all the roots of the polynomial $(x^2 - 2)(x^2 - 3)$ to be in the extension. Such a case is covered in the following definition.

Definition 2.12 $F(\alpha_1, \alpha_2, \ldots, \alpha_n)$

Let E be an extension of a field F and let $\{\alpha_1, \alpha_2, \ldots, \alpha_n\} \subseteq E$. We denote by $F(\alpha_1, \alpha_2, \ldots, \alpha_n)$ the smallest subfield of E (with respect to inclusion) that contains both F and $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$.

The field $F(\alpha_1, \alpha_2, \ldots, \alpha_n)$ can be obtained by iterating the one-element extensions defined in Definition 2.10. The next proposition shows how to do this for $n = 2$ only; you are invited to prove the corresponding statement for an arbitrary positive integer n by induction.

Proposition 2.13

Let E be an extension of a field F and let $\alpha_1, \alpha_2 \in E$. Then $F(\alpha_1, \alpha_2) = (F(\alpha_1))(\alpha_2)$.

Proof The statement follows from the fact that $F(\alpha_1, \alpha_2)$ is the smallest subfield of E containing F and $\{\alpha_1, \alpha_2\}$, and $(F(\alpha_1))(\alpha_2)$ is the smallest subfield of E containing $F(\alpha_1)$ and α_2. ■

The next definition introduces the appropriate terminology for different kinds of extensions of the form $F(\alpha)$.

Definition 2.14 *Algebraic and transcendental extension*

An extension $F(\alpha)$ of a field F is called an **algebraic extension** if α is an algebraic element over F. Analogously, $F(\alpha)$ is called a **transcendental extension** if α is transcendental over F.

The next proposition enables us to generalise the definition of algebraic extension.

Proposition 2.15

Let E be an extension of a field F and let $\alpha \in E$ be algebraic over F. Let $\beta \in F(\alpha)$. Then β is algebraic over F.

Proof Since α is algebraic over F, there is a polynomial $p(\alpha) \in F[x]$ of degree n, say, such that $p(\alpha) = 0$. The equation $p(\alpha) = 0$ expresses a linear dependence among the elements $1, \alpha, \alpha^2, \ldots, \alpha^n$, which implies that $S = \{1, \alpha, \alpha^2, \ldots, \alpha^n\}$ is a linearly dependent set in the vector space $F(\alpha)$ over F. By Definition 2.10, every element of $F(\alpha)$ is of the form $a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_r\alpha^r$ for some $r \geq 0$, where $a_i \in F$ for all i, $0 \leq i \leq r$. We conclude that S is a spanning set for $F(\alpha)$ as a vector space over F.

It follows that there is a subset B of S that is a basis for $F(\alpha)$ over F. In particular, $F(\alpha)$ is a finite-dimensional extension of F. Suppose that $[F(\alpha) : F] = m$ and consider an element $\beta \in F(\alpha)$. Then by Theorem 2.7 $\{1, \beta, \ldots, \beta^m\}$ is a linearly dependent set, so there exist $b_i \in F$, for $0 \leq i \leq m$, such that $b_0 + b_1\beta + \cdots + b_m\beta^m = 0$ and not all the b_i are zero. Hence β is algebraic over F, as required. ■

Proposition 2.15 prompts the following definition for arbitrary extensions of fields.

Definition 2.16 *Algebraic and transcendental extension (general)*

An extension E of a field F is called an **algebraic extension** if every element in E is algebraic over F. Otherwise (that is, if E contains a transcendental element), the extension is called **transcendental**.

It is important to observe that Proposition 2.15 means that this definition is consistent with Definition 2.14.

You have already encountered both algebraic and transcendental extensions. The next example revisits some of them.

Example 2.17 *Algebraic and transcendental field extensions*

The fields $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(i)$ are both algebraic extensions of $\mathbb{Q}$. The field $\mathbb{Z}_7[x]/\langle x^2-3\rangle$ in Example 1.6(b) is an algebraic extensions of $\mathbb{Z}_7$, the field $\mathbb{Q}[x]/\langle x^2-x-1\rangle$ in Exercise 1.2 is an algebraic extension of $\mathbb{Q}$, and the fields $\mathbb{Z}_{13}[x]/\langle x^2-2\rangle$ and $\mathbb{Z}_{13}[x]/\langle x^2-5\rangle$ in Worked Exercise 1.8 are algebraic extensions of $\mathbb{Z}_{13}$.

Example 2.18 *The transcendental extensions $\mathbb{Q}(e)$ and $\mathbb{Q}(\pi)$*

As a consequence of some results in advanced mathematical analysis, the Euler number e and the number π are real numbers that are not roots of any polynomial with rational coefficients. In our terminology, e and π are transcendental over $\mathbb{Q}$, so the extensions $\mathbb{Q}(e)$ and $\mathbb{Q}(\pi)$ are transcendental.

Charles Hermite proved that e is transcendental in 1873, and in 1882 Ferdinand von Lindemann proved that π is transcendental by showing that e^q is transcendental for every non-zero algebraic number q. Since then, alternative proofs of the transcendence of these two numbers have been found.

2.3 Algebraic extensions

This subsection investigates algebraic extensions in more detail. First we show that we can construct an algebraic extension of a field F from a given irreducible polynomial over F. We use Proposition 1.7 and construct the extension from the cosets in $F[x]/\langle p(x)\rangle$, and we identify the elements of F with the cosets $k+\langle p(x)\rangle$ for $k\in F$.

Consider an irreducible polynomial $p(x)$ of degree n over a field F. In Proposition 1.7 you saw that the elements of the field $E=F[x]/\langle p(x)\rangle$ may be represented as $a_0+a_1\alpha+\cdots+a_{n-1}\alpha^{n-1}$, where $\alpha=x+\langle p(x)\rangle$ and $a_0,a_1,\ldots,a_{n-1}\in F$. Recall that, in this representation, addition in E is given by

$$\begin{aligned}(a_0+a_1\alpha+\cdots+a_{n-1}\alpha^{n-1})+(b_0+b_1\alpha+\cdots+b_{n-1}\alpha^{n-1})\\ =a_0+b_0+(a_1+b_1)\alpha+\cdots+(a_{n-1}+b_{n-1})\alpha^{n-1},\end{aligned}$$

and multiplication is given by

$$(a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1})(b_0 + b_1\alpha + \cdots + b_{n-1}\alpha^{n-1}) \\ = (r_0 + r_1\alpha + \cdots + r_{n-1}\alpha^{n-1}),$$

where $r(x) = r_0 + r_1x + \cdots + r_{n-1}x^{n-1}$ is the remainder when the product $(a_0 + a_1x + \cdots + a_{n-1}x^{n-1})(b_0 + b_1x + \cdots + b_{n-1}x^{n-1})$ is divided by $p(x)$ in $F[x]$.

Regarding E as a vector space over F gives us substantial information about the extension E of F.

Theorem 2.19

Let F be a field and let $p(x)$ be an irreducible polynomial of degree n in $F[x]$. Let $E = F[x]/\langle p(x)\rangle$ and let $\alpha = x + \langle p(x)\rangle$. Let us represent E in the form $E = \{a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} : a_0, a_1, \ldots, a_{n-1} \in F\}$. Then:

(a) E is an extension of F

(b) $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$ is a basis for E as a vector space over F

(c) the degree $[E : F]$ of the field extension E over F is n

(d) $p(\alpha) = 0$

(e) $E = F(\alpha)$ and it is an algebraic extension over F.

Proof

(a) The subfield $\{a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} : a_0 \in F, a_1 = \cdots = a_{n-1} = 0\}$ of E may be identified with F, which shows that E is an extension of F.

(b) Consider the set $B = \{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$ and regard E as a vector space over F. Because of our chosen representation of E, B is a spanning set.

Suppose that

$$a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} = 0 \in E\,.$$

This is equivalent to writing

$$a_0 + a_1(x + \langle p(x)\rangle) + \cdots + a_{n-1}(x + \langle p(x)\rangle)^{n-1} = 0 \in E\,,$$

which is the same as

$$a_0 + a_1x + \cdots + a_{n-1}x^{n-1} + \langle p(x)\rangle = 0 \in E\,,$$

or, equivalently,

$$a_0 + a_1x + \cdots + a_{n-1}x^{n-1} \in \langle p(x)\rangle\,.$$

But $\deg p(x) = n$, so the only polynomial of degree lower than n in $\langle p(x)\rangle$ is the zero polynomial. Therefore

$$a_0 + a_1x + \cdots + a_{n-1}x^{n-1} = 0 \in F[x]\,.$$

But this means that $a_0 = a_1 = \cdots = a_{n-1} = 0$.

In the language of vector spaces, we have shown that B is also a linearly independent set. Thus B is a basis for E as a vector space over F.

(c) By part (b), B is a basis for E as a vector space over F, and so $[E : F] = n$.

(d) This follows from Proposition 1.7.

(e) This follows from the fact that every element of E can be written in the form $a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1}$ for suitable $a_0, a_1, \ldots, a_{n-1} \in F$, and from $p(\alpha) = 0$. ■

The algebraic extension $F(\alpha)$ of F described in Theorem 2.19 is sometimes said to be obtained by **adjoining** α to F.

We can use Theorem 2.19 to show that for any non-constant polynomial $f(x)$, not necessarily irreducible, over a field F, we can construct an extension of F that contains a root of $f(x)$.

Corollary 2.20

Let F be a field and let $f(x)$ be a non-constant polynomial in $F[x]$. Then there is an extension E of F that contains an element α such that $f(\alpha) = 0$.

Proof Since $f(x)$ is not a constant, there is an irreducible polynomial $h(x) \in F[x]$ such that $f(x) = h(x)g(x)$ for some $g(x) \in F[x]$. By Theorem 2.19, there are an extension E of F and an element $\alpha \in E$ such that $h(\alpha) = 0$. Since $f(x) = h(x)g(x)$, $f(\alpha) = 0$, and so E is the required extension of F. ■

We will now reverse our line of thought and show that one can start with an algebraic element α in an extension E of a field F and find an irreducible polynomial that gives rise to the extension $F(\alpha)$.

Theorem 2.21

Let E be an extension of a field F and suppose that $\alpha \in E \backslash F$ is algebraic over F. Then:

(a) there is an irreducible polynomial $h(x) \in F[x]$ such that $h(\alpha) = 0$ and $F[x]/\langle h(x)\rangle \cong F(\alpha)$

(b) there is a unique irreducible monic polynomial $m(x) \in F[x]$ such that $m(\alpha) = 0$ and $F[x]/\langle m(x)\rangle \cong F(\alpha)$

(c) $[F(\alpha) : F] = \deg m(x) = \deg h(x)$.

Proof

(a) Since α is algebraic over F, there is a polynomial $h(x)$ such that $h(\alpha) = 0$. If $h(x)$ is reducible, it can be written as a product $h_1(x)h_2(x)$ where both $h_1(x)$ and $h_2(x)$ have lower degree than $h(x)$. Since $h(\alpha) = 0$, either $h_1(\alpha) = 0$ or $h_2(\alpha) = 0$. Since this process must stop, we can assume, without loss of generality, that $h(x)$ is irreducible.

Let $f_\alpha : F[x] \to F(\alpha)$ be the evaluation mapping, which is defined by $f_\alpha(r(x)) = r(\alpha)$ for every polynomial $r(x) \in F[x]$. This map can be shown to be a homomorphism by an argument similar to the solution to Exercise 4.7 of Chapter 17 and the discussion following it. This homomorphism is onto, since every element of $F(\alpha)$ can be expressed as a finite sum of elements of the form $c\alpha^k$ and so can be written in the form $f_\alpha(s(x))$ for some polynomial $s(x) \in F[x]$.

To complete the proof, we need to show that $\mathrm{Ker}(f_\alpha) = \langle h(x)\rangle$. It is clear that $\langle h(x)\rangle \subseteq \mathrm{Ker}(f_\alpha)$, since $h(\alpha) = 0$ and so any polynomial in $\langle h(x)\rangle$ must map to 0. Since $h(x)$ is irreducible, we know from Theorem 4.22 of Chapter 17 that $\langle h(x)\rangle$ is a maximal ideal. Hence $\langle h(x)\rangle = \mathrm{Ker}(f_\alpha)$ and so by the First Isomorphism Theorem for rings we have $F[x]/\langle h(x)\rangle \cong F(\alpha)$.

(b) Let $m(x) = ah(x)$ where a is the inverse of the leading coefficient of $h(x)$. Then $m(x)$ is monic and irreducible and $\langle m(x)\rangle = \langle h(x)\rangle$. It remains to show that $m(x)$ is unique.

Suppose that $g(x)$ is a monic irreducible polynomial with $g(\alpha) = 0$ and such that $F[x]/\langle g(x)\rangle \cong F(\alpha)$. Then it follows from Theorem 2.19 that

$$\deg g(x) = [F(\alpha) : F] = \deg m(x)\,.$$

Since both $g(x)$ and $m(x)$ are monic polynomials, the polynomial $k(x) = g(x) - m(x)$ has lower degree and satisfies $k(\alpha) = 0$. This is only possible if $k(x)$ is the zero polynomial, that is, if $g(x) = m(x)$ as required.

(c) This follows directly from Theorem 2.19. ■

The result of Theorem 2.21(b) suggests making the following definition.

Definition 2.22 *Minimal polynomial*

Let E be an extension of a field F and suppose that $\alpha \in E\backslash F$ is algebraic over F. A non-zero polynomial $h(x) \in F[x]$ is called the **minimal polynomial** for α if it is monic and a polynomial of lowest degree in $F[x]$ such that $h(\alpha) = 0$.

By Theorem 2.21(b), for each $\alpha \in E$ there is a unique minimal polynomial for α, so we refer to *the* minimal polynomial of an algebraic element over a field.

The next exercise clarifies the relation between irreducible monic polynomials and minimal polynomials.

Exercise 2.2

Let E be an extension of a field F and suppose that $\alpha \in E \backslash F$ is algebraic over F. Let $h(x)$ be a monic polynomial that is irreducible over F and such that $h(\alpha) = 0$. Show that $h(x)$ is the minimal polynomial for α.

The solution to Exercise 2.2 enables us to prove the following corollary to Theorem 2.21, where we define a field extension starting from an irreducible polynomial rather than from an algebraic element.

Corollary 2.23

Let E be an extension of a field F and suppose that $h(x)$ is an irreducible polynomial in $F[x]$ and that $\alpha \in E$ with $h(\alpha) = 0$. Then $F(\alpha) \cong F[x]/\langle h(x) \rangle$.

Proof Let $m(x)$ be the polynomial obtained by dividing $h(x)$ through by the leading coefficient. Then $m(x)$ is monic and irreducible and $m(\alpha) = 0$. Then, by the solution to Exercise 2.2, $m(x)$ is the minimal polynomial for α. Since $\langle m(x) \rangle = \langle h(x) \rangle$ the result follows by Theorem 2.21. ■

The next exercise asks you to practise calculating minimal polynomials of algebraic elements and looking at the corresponding extensions.

Exercise 2.3

(a) Write down the minimal polynomial for $i = \sqrt{-1}$ over $\mathbb{Q}$.

(b) Let $E = \mathbb{Z}_5(\alpha)$ where $\alpha^2 = 2$ and $F = \mathbb{Z}_5(\beta)$ where $\beta^2 = 3$.

(i) Write down the minimal polynomials for α and β.

(ii) Show that $\alpha \in \mathbb{Z}_5(\beta)$ so that $\mathbb{Z}_5(\alpha) = \mathbb{Z}_5(\beta)$.

Exercise 2.3(b) demonstrates that the same extension can be obtained by adjoining elements with different minimal polynomials.

Exercise 2.4

Let α be a root of the polynomial $x^3 - 3x - 1$. Find the degree of the extension $\mathbb{Q}(\alpha)$ over $\mathbb{Q}$.

Exercise 2.5

Let E be an extension of a field F and let $h(x)$ be an irreducible polynomial over F, and let $\alpha, \beta \in E$ be roots of $h(x)$. Show that $F(\alpha) \cong F(\beta)$.

It is not always the case that algebraic extensions of the same degree are isomorphic. The next worked exercise illustrates this fact.

Worked Exercise 2.24

Show that the fields $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt{5})$ are not isomorphic.

Solution

Suppose, by way of contradiction, that $\phi\colon\ \mathbb{Q}(\sqrt{2}) \to \mathbb{Q}(\sqrt{5})$ is an isomorphism. Since both fields are subfields of $\mathbb{C}$, we know from Theorem 1.14 that $\phi(x) = x$ for all $x \in \mathbb{Q}$. In particular $\phi(2) = 2$.

Now the image of the element $\sqrt{2} \in \mathbb{Q}(\sqrt{2})$ under ϕ must have the form $r + s\sqrt{5}$ for some $r, s \in \mathbb{Q}$. Applying ϕ to both sides of the equation $2 = \sqrt{2}\sqrt{2}$ gives

$$2 = \phi(2) = \phi(\sqrt{2}\sqrt{2}) = \phi(\sqrt{2})\phi(\sqrt{2}) = (r + s\sqrt{5})^2,$$

which implies that $2 = r^2 + 5s^2 + 2rs\sqrt{5}$.

Since the set $\{1, \sqrt{5}\}$ is a basis for $\mathbb{Q}(\sqrt{5})$, we can compare coefficients and deduce that $r^2 + 5s^2 = 2$ and $rs = 0$. If $rs = 0$ then either $s = 0$, so that $2 = r^2$, which contradicts the fact that $r \in \mathbb{Q}$, or $r = 0$, so that $2 = 5s^2$, contrary to the fact that $s \in \mathbb{Q}$.

We conclude that the fields $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt{5})$ are not isomorphic.

The next exercise elaborates on Worked Exercise 2.24 to illustrate a case where two extensions of a finite field are isomorphic.

Worked Exercise 2.25

ξ is the Greek letter 'xi'.

Consider the algebraic extensions $\mathbb{Z}_3(\xi)$, where $\xi^2 + \xi + 2 = 0$, and $\mathbb{Z}_3(i)$, where $i^2 + 1 = 0$.

(a) Write down the successive powers of ξ in terms of the basis $\{1, \xi\}$.

(b) Find an isomorphism between the two fields.

Solution

(a) The equation $\xi^2 + \xi + 2 = 0$ and arithmetic in $\mathbb{Z}_3(\xi)$ give $\xi^2 = 1 - \xi$, $\xi^3 = -1 - \xi$, $\xi^4 = -1$, $\xi^5 = -\xi$, $\xi^6 = \xi - 1$, $\xi^7 = 1 + \xi$, $\xi^8 = 1$. Since $\{1, \xi\}$ is a basis and $|\mathbb{Z}_3| = 3$, we know that $|\mathbb{Z}_3(\xi)| = 9$, so the multiplicative group of non-zero elements of $\mathbb{Z}_3(\xi)$ has 8 elements. It follows that ξ generates this group.

(b) We give three possible solutions.

(i) Suppose ϕ is a map from $\mathbb{Z}_3(i)$ to $\mathbb{Z}_3(\xi)$ such that $\phi(i) = a + b\xi$. Applying ϕ to $-1 = i^2$ gives

$$\begin{aligned} -1 = \phi(i^2) = (\phi(i))^2 &= (a + b\xi)^2 \\ &= a^2 + 2ab\xi + b^2\xi^2 \\ &= a^2 + 2ab\xi + b^2(1 - \xi) \\ &= a^2 + b^2 + (2a - b)b\xi, \end{aligned}$$

which implies $a^2 + b^2 = -1$ and $(2a - b)b = 0$.

From the second of these equations we deduce that either $b = 0$ or $b = -a$. If $b = 0$ the first equation reduces to $a^2 = -1$, which has no solutions mod 3. If $b = -a$ the first equation reduces to $a^2 = 1$, which has two solutions $a = 1$ and $a = -1$. We take the second of these, so $b = 1 = -a$, and define $\phi(i) = -1 + \xi$.

Thus, we have obtained a map from $\mathbb{Z}_3(i)$ to $\mathbb{Z}_3(\xi)$ defined by $\phi(a + bi) = a + b(-1 + \xi) = a - b + b\xi$. We check that ϕ is a field isomorphism. The map is an additive homomorphism, because

$$\begin{aligned} \phi(a + bi + c + di) &= \phi((a + c) + (b + d)i) \\ &= a + c - (b + d) + (b + d)\xi \\ &= (a - b) + b\xi + (c - d) + d\xi \\ &= \phi(a + bi) + \phi(c + di). \end{aligned}$$

We show that the map ϕ is a multiplicative homomorphism. On the one hand,

$$\begin{aligned} \phi((a + bi)(c + di)) &= \phi(ac - bd + (ad + bc)i) \\ &= (ac - bd - ad - bc) + (ad + bc)\xi. \end{aligned}$$

On the other hand, we have

$$\begin{aligned} \phi(a + bi)\phi(c + di) &= (a - b + b\xi)(c - d + d\xi) \\ &= (a - b)(c - d) + (b(c - d) \\ &\quad + d(a - b))\xi + bd\xi^2 \\ &= (a - b)(c - d) + bd + (b(c - d) \\ &\quad + d(a - b) - bd)\xi \\ &= ac - ad - bc - bd + (bc + ad)\xi. \end{aligned}$$

Therefore

$$\phi((a + bi)(c + di)) = \phi(a + bi)\phi(c + di).$$

Since ϕ is onto and the fields have the same cardinality, ϕ is an isomorphism.

(ii) For our second solution, we observe that any isomorphism between the two fields must take an element of multiplicative order 8 to an element of the same order, so we define $\psi(1+i) = \xi$. This implies that

$$1 + \psi(i) = \xi, \quad \text{or, equivalently,} \quad \psi(i) = \xi - 1, \quad \text{and}$$
$$\psi(a+bi) = a + b(\xi - 1) = a - b + b\xi,$$

obtaining the same candidate for an isomorphism of the fields as in solution (i). The proof is concluded as in the first solution.

(iii) A third solution is obtained by proving that the two extensions are, in fact, equal. We observe that

$$(1-i)^2 + (1-i) + 2 = -2i + (1-i) + 2 \equiv 0 \pmod 3,$$

so that there is a solution of $\xi^2 + \xi + 2 = 0$ in $\mathbb{Z}_3(i)$. This shows that $\mathbb{Z}_3(\xi) \subseteq \mathbb{Z}_3(i)$. Since $[\mathbb{Z}_3(i) : \mathbb{Z}_3] = 2$ and there is no solution to $\xi^2 + \xi + 2 = 0$ in $\mathbb{Z}_3$, this is only possible if $\mathbb{Z}_3(\xi) = \mathbb{Z}_3(i)$. Hence the two extensions are not just isomorphic, but equal.

In Corollary 2.23 you saw that extensions of a field obtained by adjoining a different root of the same irreducible polynomials are isomorphic, no matter which root one chooses. The next example shows that the extensions, although isomorphic, need not be equal to each other.

Example 2.26 *Distinct isomorphic field extensions*

Consider the field $\mathbb{Q}$ and the polynomial $x^3 - 2 \in \mathbb{Q}[x]$. By Theorem 2.19 we know that there exists an extension $\mathbb{Q}(\alpha)$ of $\mathbb{Q}$ with $\alpha^3 - 2 = 0$. Since $x^3 - 2$ is monic and irreducible over $\mathbb{Q}$, we know that $x^3 - 2$ is the minimal polynomial for α. We also know that

$$x^3 - 2 = (x - \sqrt[3]{2})(x - \omega\sqrt[3]{2})(x - \omega^2\sqrt[3]{2}),$$

where $\omega = e^{2\pi i/3}$. Note that $\omega^2 + \omega + 1 = 0$. How is α related to $\sqrt[3]{2}$, $\omega\sqrt[3]{2}$ and $\omega^2\sqrt[3]{2}$?

The answer is that α could, in fact, be any of these three elements, and by Corollary 2.23 we have

$$\mathbb{Q}(\alpha) \cong \mathbb{Q}(\sqrt[3]{2}) \cong \mathbb{Q}(\omega\sqrt[3]{2}) \cong \mathbb{Q}(\omega^2\sqrt[3]{2}) \cong \mathbb{Q}[x]/\langle x^3 - 2\rangle.$$

However, the fact that the three fields are isomorphic does not imply that they are identical. Indeed, we will show this is not the case.

We begin by observing that $\omega \notin \mathbb{R}$ but $\sqrt[3]{2} \in \mathbb{R}$. It follows that, although $\mathbb{Q}(\sqrt[3]{2}) \cong \mathbb{Q}(\omega\sqrt[3]{2})$, the two fields are not identical.

Now suppose that $\mathbb{Q}(\omega\sqrt[3]{2}) = \mathbb{Q}(\omega^2\sqrt[3]{2})$. Multiplying the equation $\omega^2 + \omega + 1 = 0$ by $\sqrt[3]{2}$ and rearranging terms gives

$$\omega^2\sqrt[3]{2} = -\omega\sqrt[3]{2} - \sqrt[3]{2}.$$

This equation shows that if $\omega^2\sqrt[3]{2} \in \mathbb{Q}(\omega\sqrt[3]{2})$, then also $\sqrt[3]{2} \in \mathbb{Q}(\omega\sqrt[3]{2})$. This would mean that $\mathbb{Q}(\sqrt[3]{2}) \subseteq \mathbb{Q}(\omega\sqrt[3]{2})$ and so, since both extensions have degree 3 over $\mathbb{Q}$ we would have $\mathbb{Q}(\sqrt[3]{2}) = \mathbb{Q}(\omega\sqrt[3]{2})$, which is not the case. Hence the extensions $\mathbb{Q}(\omega\sqrt[3]{2})$ and $\mathbb{Q}(\omega^2\sqrt[3]{2})$ are distinct.

Thus we have shown that $\mathbb{C}$ contains three isomorphic fields that are extensions of degree 3 over $\mathbb{Q}$ and that contain a root of the polynomial $x^3 - 2$. As you will see in Section 4, we can go a step further by noting that $x^2 + x + 1$ is an irreducible polynomial in $\mathbb{Q}(\sqrt[3]{2})[x]$ and by considering a further algebraic extension to obtain $\mathbb{Q}(\sqrt[3]{2}, \omega)$.

The next three exercises offer you a chance to try computations with field extensions.

Exercise 2.6

Prove that the six fields $\mathbb{Z}_{13}(\sqrt{t})$ for $t \in \{\pm 2, \pm 5, \pm 6\}$ are mutually isomorphic.

Exercise 2.7

Show that the fields $\mathbb{Q}(i)$ and $\mathbb{Q}(j)$, where j is a root of $x^2 - 2x + 2$, are isomorphic.

Exercise 2.8

Show that the fields $\mathbb{Q}(\xi)$ with $\xi^2 = -2$ and $\mathbb{Q}(\eta)$, where η satisfies $x^2 - 2x - 2 = 0$, cannot be isomorphic.

η is the Greek letter 'eta'

Exercises 2.7 and 2.8 asked you to work with some algebraic extensions of the field $\mathbb{Q}$ of rational numbers. In this setting, it is quite natural to ask when two extensions of $\mathbb{Q}$, each obtained by adjoining the square root of a rational number, are isomorphic.

Theorem 2.27

Let t_1 and t_2 be positive rational numbers such that both $\sqrt{t_1}$ and $\sqrt{t_2}$ are irrational. Then the fields $\mathbb{Q}(\sqrt{t_1})$ and $\mathbb{Q}(\sqrt{t_2})$ are isomorphic if, and only if, there exists a rational number s such that $t_1 = s^2 t_2$.

Proof We can write the elements of $\mathbb{Q}(\sqrt{t_1})$ and $\mathbb{Q}(\sqrt{t_2})$ as $a + b\sqrt{t_1}$ and $c + d\sqrt{t_2}$ respectively.

Suppose that $\phi : \mathbb{Q}(\sqrt{t_1}) \to \mathbb{Q}(\sqrt{t_2})$ is an isomorphism, and suppose further that $\phi(\sqrt{t_1}) = r + s\sqrt{t_2}$ for some $r, s \in \mathbb{Q}$. Since t_1 is rational, we have

$$t_1 = \phi(t_1) = \phi(\sqrt{t_1}\sqrt{t_1}) = \phi(\sqrt{t_1})\phi(\sqrt{t_1}) = (r + s\sqrt{t_2})^2,$$

which gives

$$t_1 = r^2 + t_2 s^2 + 2rs\sqrt{t_2}.$$

Since t_1 is non-zero, at least one of r, s is non-zero. If $rs \neq 0$, then the last equation gives $\sqrt{t_2} = \frac{t_1 - r^2 - t_2 s^2}{2rs}$, which expresses the irrational number $\sqrt{t_2}$ by a rational number, a contradiction. If $s = 0$, then the equation for t_1 collapses to $t_1 = r^2$, which contradicts the fact that $r \in \mathbb{Q}$. Thus $r = 0$, and the equation for t_1 reduces to $t_1 = s^2 t_2$ as required.

On the other hand, if $t_1 = s^2 t_2$ then $a + b\sqrt{t_1} = a + bs\sqrt{t_2}$ and so $\mathbb{Q}(\sqrt{t_1}) = \mathbb{Q}(\sqrt{t_2})$, that is, the fields $\mathbb{Q}(\sqrt{t_1})$ and $\mathbb{Q}(\sqrt{t_2})$ are not only isomorphic but, in fact, identical. ■

The next exercise illustrates Theorem 2.27.

Exercise 2.9

(a) Show that $\mathbb{Q}(\sqrt{2}) \cong \mathbb{Q}(-\sqrt{2})$.

(b) Show that $\mathbb{Q}(\sqrt{2}) \ncong \mathbb{Q}(\sqrt{-2})$.

In order to achieve a higher level of generality in the theory of field extensions, let us show that the isomorphism of two field extensions obtained by adjoining roots of an irreducible polynomial carries over to the case where the underlying fields are isomorphic (rather than equal). We will need such a general result in Section 4, where we consider fields containing all the roots of a given polynomial.

Theorem 2.28

Let F_1, F_2 be fields. Let $\phi : F_1 \to F_2$ be a field isomorphism and let $\hat{\phi}$ be the homomorphism $\hat{\phi} : F_1[x] \to F_2[x]$ that extends ϕ to $F_1[x]$, so that

$$\hat{\phi}(a_0 + a_1 x + \cdots + a_n x^n) = \phi(a_0) + \phi(a_1)x + \cdots + \phi(a_n)x^n.$$

Let $h_1(x)$ be an irreducible polynomial over F_1 and let $h_2(x) = \hat{\phi}(h_1(x))$ be its (irreducible) image under the mapping $\hat{\phi}$. Let α_1 be a root of $h_1(x)$ and let α_2 be a root of $h_2(x)$. Then the fields $F_1(\alpha_1)$ and $F_2(\alpha_2)$ are isomorphic.

Proof From Corollary 2.23 it follows that $F_1(\alpha_1) \cong F_1[x]/\langle h_1(x)\rangle$ and $F_2(\alpha_2) \cong F_2[x]/\langle h_2(x)\rangle$. Let $\theta : F_2[x] \to F_2[x]/\langle h_2(x)\rangle$ be the natural homomorphism and let σ be the composition $\theta \circ \hat{\phi}$. Then, for every $g(x) \in F_1(x)$ we have $\sigma(g(x)) = \hat{\phi}(g(x)) + \langle h_2(x)\rangle$.

Now,

$$\begin{aligned}\mathrm{Ker}(\sigma) &= \{g(x) : \hat{\phi}(g(x)) \in \langle h_2(x)\rangle\}\\ &= \{g(x) : \hat{\phi}(g(x)) = a(x)h_2(x) \text{ for some } a(x) \in F_2[x]\}\\ &= \{g(x) : g(x) = (\hat{\phi})^{-1}(a(x)h_2(x)) \text{ for some } a(x) \in F_2[x]\}\\ &= \{g(x) : g(x) = b(x)h_1(x) \text{ for some } b(x) \in F_1[x]\}\\ &= \langle h_1(x)\rangle.\end{aligned}$$

Thus, by the First Isomorphism Theorem,

$$F_1[x]/\langle h_1(x)\rangle \cong \mathrm{Im}\,\sigma = F_2[x]/\langle h_2(x)\rangle$$

and so, by Theorem 2.19, $F_1(\alpha_1) \cong F_2(\alpha_2)$ as required. ■

The final theorem in this subsection enables us to find a basis for extensions obtained by adjoining more than one element. Although the proof looks long, the idea is straightforward – namely, forming a basis from the products of elements of the bases of extensions of lower degree.

Theorem 2.29 *The KLM Theorem for field extensions*

Let K, L and M be fields such that $K \subset L \subset M$ and let the degrees $[M : L]$ and $[L : K]$ be both finite. Then

$$[M : L][L : K] = [M : K].$$

Proof We use the fact that extensions can be regarded as vector spaces over the smaller fields.

Since the degree $[M : L]$ is finite, say, equal to m, the vector space M has a basis $B_M = \{\alpha_1, \alpha_2, \ldots, \alpha_m\}$ over the field L. That is, the set B_M is linearly independent over L and generates M, which means that every element γ of M can be written as a linear combination

$$\gamma = c_1\alpha_1 + c_2\alpha_2 + \cdots + c_m\alpha_m \tag{1}$$

where $c_j \in L$, $1 \leq j \leq m$.

By the same token, since the degree $[L : K]$ is finite, say equal to n, the vector space L has a basis $B_L = \{\beta_1, \beta_2, \ldots, \beta_n\}$ over the field K. As above, this means that the set B_L is linearly independent over the field K and generates L, that is, every element of L can be written as a linear combination of elements in B_L. In particular, this is true for any of the elements $c_1, c_2, \ldots, c_m$. That is, for every $j = 1, 2, \ldots, m$ we have

$$c_j = c_{j1}\beta_1 + c_{j2}\beta_2 + \cdots + c_{jn}\beta_n \tag{2}$$

where $c_{jk} \in K$ for all j, k such that $1 \leq j \leq m$ and $1 \leq k \leq n$.

Substituting the equations (2) in (1) for each $k = 1, 2, \ldots, n$ gives

$$\begin{aligned}\gamma = \quad & c_{11}\alpha_1\beta_1 + c_{12}\alpha_1\beta_2 + \cdots + c_{1n}\alpha_1\beta_n \\ & + c_{21}\alpha_2\beta_1 + c_{22}\alpha_2\beta_2 + \cdots + c_{2n}\alpha_2\beta_n \\ & + \cdots \\ & + c_{m1}\alpha_m\beta_1 + c_{m2}\alpha_m\beta_2 + \cdots + c_{mn}\alpha_m\beta_n\end{aligned}$$

where $c_{jk} \in K$, $1 \leq j \leq m$, $1 \leq k \leq n$.

This shows that the field M as a vector space over K is generated by the mn elements $\alpha_j\beta_k$, where $1 \leq j \leq m$ and $1 \leq k \leq n$.

We conclude the proof by showing that the mn elements $\alpha_j\beta_k$ with $1 \leq j \leq m$ and $1 \leq k \leq n$ are linearly independent over K. Suppose that

$$\begin{aligned}0 = \quad & d_{11}\alpha_1\beta_1 + d_{12}\alpha_1\beta_2 + \cdots + d_{1n}\alpha_1\beta_n \\ & + d_{21}\alpha_2\beta_1 + d_{22}\alpha_2\beta_2 + \cdots + d_{2n}\alpha_2\beta_n \\ & + \cdots \\ & + d_{m1}\alpha_m\beta_1 + d_{m2}\alpha_m\beta_2 + \cdots + d_{mn}\alpha_m\beta_n\end{aligned}$$

for some $d_{jk} \in K$, $1 \leq j \leq m$, $1 \leq k \leq n$. Re-grouping the elements gives

$$\begin{aligned}0 = \quad & (d_{11}\beta_1 + d_{12}\beta_2 + \cdots + d_{1n}\beta_n)\alpha_1 \\ & + (d_{21}\beta_1 + d_{22}\beta_2 + \cdots + d_{2n}\beta_n)\alpha_2 \\ & + \cdots \\ & + (d_{m1}\beta_1 + d_{m2}\beta_2 + \cdots + d_{mn}\beta_n)\alpha_m.\end{aligned}$$

This equality expresses 0 as a linear combination of vectors $\alpha_1, \alpha_2, \ldots, \alpha_m$ in M, with coefficients in L. Since the set $\alpha_1, \alpha_2, \ldots, \alpha_m$ is linearly independent over L, we conclude that

$$\begin{aligned}0 &= d_{11}\beta_1 + d_{12}\beta_2 + \cdots + d_{1n}\beta_n \\ 0 &= d_{21}\beta_1 + d_{22}\beta_2 + \cdots + d_{2n}\beta_n \\ &\cdots \\ 0 &= d_{m1}\beta_1 + d_{m2}\beta_2 + \cdots + d_{mn}\beta_n.\end{aligned}$$

For each j such that $1 \leq j \leq m$, the jth equality above expresses 0 as a linear combination of vectors $\beta_1, \beta_2, \ldots, \beta_n$ in L with coefficients d_{jk} in K. Since the vectors $\beta_1, \beta_2, \ldots, \beta_n$ are linearly independent over K, we conclude that $d_{jk} = 0$ for all j, k such that $1 \leq j \leq m$ and $1 \leq k \leq n$.

Thus, the set $\{\alpha_j\beta_k : \ 1 \leq j \leq m, \ 1 \leq k \leq n\}$ is indeed a basis for M. It follows that the degree of M over K is mn, and hence $[M : L][L : K] = [M : K]$, as claimed. ■

Because of the symbols appearing in its formulation, this result is sometimes nicknamed the 'Royal Dutch Airlines' or 'KLM' Theorem.

Exercise 2.10

Let $L = \mathbb{Q}(\sqrt{2})$. Show that $x^2 - 3$ is irreducible over L, that is, show that there are no $a, b \in \mathbb{Q}$ such that $(a + b\sqrt{2})^2 = 3$. What is $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}]$?

2.4 Transcendental extensions

Subsection 2.3 presented a selection of basic results concerning the structure of algebraic extensions. This subsection focuses on the structure of transcendental extensions. Recall that if E is an extension of a field F, an element $\alpha \in E \backslash F$ is said to be transcendental over F if α is not a root of any polynomial over F.

Theorem 2.30

Let E be an extension of a field F and let $\alpha \in E$ be a transcendental element over F. Then the smallest subfield $F(\alpha)$ of E containing F and α has the form

$$F(\alpha) = \{f(\alpha)(g(\alpha))^{-1} : \ f(x), g(x) \in F[x], \ g(x) \neq 0\}.$$

That is, $F(\alpha)$ is isomorphic to the field of fractions of the integral domain $F[x]$.

Proof The evaluation at α of a polynomial $g(x) \in F[x]$, that is, the value $g(\alpha)$, belongs to $F(\alpha)$ since it consists of sums and products of elements of F and powers of α. Note that, since α is transcendental, $g(\alpha)$ is non-zero if $g(x)$ is non-zero, and any non-zero element $g(\alpha) \in F(\alpha)$ has a multiplicative inverse $(g(\alpha))^{-1}$.

Also, for any $f(x) \in F[x]$ one may form the product $f(\alpha)(g(\alpha))^{-1}$.

Thus, if α is transcendental, the smallest subfield $F(\alpha)$ of F that contains both F and α must, at the very least, contain all the elements of the form $f(\alpha)(g(\alpha))^{-1}$, where $f(x) \in F[x]$ is any polynomial and $g(x) \in F[x]$ is a non-zero polynomial.

We now show that $F(\alpha)$ contains no other elements. In order to do so, it is sufficient to show that the set

$$F_\alpha = \{f(\alpha)(g(\alpha))^{-1} : \ f(x), g(x) \in F[x], \ g(x) \neq 0\}$$

is a subfield of E. We use the subfield criterion given in Book C, Chapter 11, Lemma 1.6.

For closure of addition we have:

$$\begin{aligned}
&f(\alpha)(g(\alpha))^{-1} + f_1(\alpha)(g_1(\alpha))^{-1} \\
&\quad = f(\alpha)(g(\alpha))^{-1} g_1(\alpha)(g_1(\alpha))^{-1} + f_1(\alpha)(g_1(\alpha))^{-1} g(\alpha)(g(\alpha))^{-1} \\
&\quad = f(\alpha) g_1(\alpha)(g(\alpha))^{-1}(g_1(\alpha))^{-1} + f_1(\alpha) g(\alpha)(g_1(\alpha))^{-1}(g(\alpha))^{-1} \\
&\quad = [f(\alpha) g_1(\alpha) + f_1(\alpha) g(\alpha)][g(\alpha)^{-1} g_1(\alpha)^{-1}] \in F_\alpha \\
&\quad = [f(\alpha) g_1(\alpha) + f_1(\alpha) g(\alpha)](g(\alpha) g_1(\alpha))^{-1} \in F_\alpha,
\end{aligned}$$

where this calculation comes from the familiar method for adding fractions. (Note the ample use of commutativity in these calculations.)

For closure of multiplication we have:

$$f(\alpha)(g(\alpha))^{-1} \times f_1(\alpha)(g_1(\alpha))^{-1} = f(\alpha) f_1(\alpha)[g(\alpha) g_1(\alpha)]^{-1} \in F_\alpha.$$

It is clear that $1 \in F_\alpha$. Moreover, if $f(\alpha)(g(\alpha))^{-1} \in F_\alpha$ and $f(x)$ is non-zero, then the multiplicative inverse $g(\alpha)(f(\alpha))^{-1}$ is also in F_α. Hence F_α is a subfield of E.

Since F_α is a field containing both F and α, it follows that $F(\alpha) \subseteq F_\alpha$. On the other hand, all the elements of F_α must be contained in $F(\alpha)$, and so $F_\alpha = F(\alpha)$.

The isomorphism with the field of fractions of polynomials over F follows from Definition 1.6 of Chapter 17. ■

We have just shown that a given transcendental extension takes a particular form. We now show, perhaps in a surprisingly brief way, that every field has a transcendental extension.

Theorem 2.31

For every field L, the field of fractions of the integral domain $L[x]$ is an extension of L that contains a transcendental element over L.

Proof Let L be an arbitrary field. Consider the ring $L[x]$ of all polynomials in the indeterminate x with coefficients in L. We know from Book C, Chapter 11, Lemma 2.8 that $L[x]$ is an integral domain. We may therefore construct the corresponding field of fractions and denote it by F.

By this construction, elements of F can be identified with fractions of the form $\frac{f(x)}{g(x)}$, where $f(x), g(x) \in L[x]$ and $g(x)$ is a non-zero polynomial.

We now claim that the polynomial $t(x) = x$ is a transcendental element of the field F over L. Indeed, suppose that $t(x)$ is a root of some non-zero polynomial $f(x) \in L[x]$ in some extension E of L. Then substituting the element $t(x) \in E$ for x into $f(x)$ would give zero, that is, $f(t(x)) = 0$ in E.

Since $t(x)$ is an element of both the fields E and F, it is also an element of the field $E \cap F$. Therefore in $E \cap F$ we have $f(t(x)) = 0$. But since $t(x) = x$, this would mean that $f(x) = 0$ in $E \cap F$; in particular, $f(x) = 0$ in F, that is, f would be a zero polynomial in $L[x]$, contrary to our assumption about $f(x)$. Thus, the element $x \in F$ is transcendental over L, as claimed. ■

Theorem 2.30 shows in particular that the extension of a field by a transcendental element is isomorphic to the field of fractions of the polynomial ring over the field. This result gives the following corollary.

Corollary 2.32

Let E be a field extension of a field F. Suppose that $\alpha, \beta \in E$ and both α and β are transcendental elements over F. Then $F(\alpha) \cong F(\beta)$.

Proof This follows directly from Theorem 2.30 since both $F(\alpha)$ and $F(\beta)$ are isomorphic to the field of fractions of $F(x)$. ■

3 Finite fields

Finite fields are an important area of study and have significant applications in digital information exchange through coding theory and cryptography.

This section begins with an investigation of the structure of the multiplicative group whose elements are the non-zero elements of a finite field. For a field F, this group is usually denoted by F^*.

3.1 The multiplicative group of a finite field

We prove that the multiplicative group of a finite field is cyclic by finding an element that has the same order as that of the group. This involves a counting argument about elements of particular orders. Recall that, by Lagrange's Theorem (Book B, Chapter 5, Theorem 2.16), the order of an element must divide the order of the group. The next exercise identifies elements of a given order within the multiplicative group.

Exercise 3.1

Let F be a finite field of order p^n for some prime p. Further, let d be a positive divisor of $p^n - 1$ and let u be an element of order d in $F^* = F\backslash\{0\}$.

The fact that every finite field has order of the form p^n follows from Theorem 2.9.

(a) Show that any element of the set $U = \{u, u^2, \ldots, u^{d-1}, 1\}$ is a root of the polynomial $x^d - 1$.

(b) Show that for $u \in U$ we have $u^i \neq u^j$ if $0 \leq i < j < d$.

In the counting argument that we are about to develop, we use the Euler ϕ-function that gives, for a positive integer $m \geq 2$, the number of positive integers smaller than m and relatively prime to m (with $\phi(1) = 1$). You encountered this function in Book C, Chapter 9, Section 3.

Lemma 3.1

Let F be a finite field of order p^n for some prime p and let d be a positive divisor of $p^n - 1$. Let a_d be the number of elements of $F^* = F\backslash\{0\}$ that have multiplicative order equal to d. If $a_d > 0$ then $a_d = \phi(d)$ where $\phi(d)$ is the value of the Euler ϕ-function at d.

There are elements of U of order dividing d but less than d. For example, 1 is such an element.

Proof If $a_d > 0$, there exists an element $u \in F^*$ of order d. By Exercise 3.1, $U = \{u, u^2, \ldots, u^{d-1}, 1\}$ is a set of d distinct roots of the polynomial $x^d - 1$ over F. By Proposition 4.3 of Book C, Chapter 11, the polynomial $x^d - 1$ has at most d roots in F. Thus, the set U contains all the roots of $x^d - 1$ in F, and hence also in F^*. It follows that all the elements of F^* of order d must lie in the set U.

The elements of U that have order *equal* to d (and not just a proper divisor of d) are the powers u^j of u such that $1 \leq j \leq d$ and j is relatively prime to d. The number of such exponents j is the value $\phi(d)$ of the Euler ϕ-function. The result follows. ■

Exercise 3.2

Let n be a positive integer and let d be a positive divisor of n. Show that all the elements of order d in the additive group $\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$ have the form sr for $r = \frac{n}{d}$, where $1 \leq s \leq d$ and s and d are relatively prime. Deduce that the number of elements of order d in the cyclic group $(\mathbb{Z}_n, +)$ is equal to the value $\phi(d)$ of the Euler ϕ-function.

We need one more auxiliary result.

Lemma 3.2

Let $q = p^n$ for some prime p and let

$$A = \{d : 0 < d < q \text{ and } d \text{ divides } q - 1\}.$$

Then $q - 1 = \sum_{d \in A} \phi(d)$, where $\phi(d)$ is the Euler ϕ-function.

Proof By Exercise 3.2, for each positive divisor d of $q - 1$ the group $\mathbb{Z}_{q-1}$ contains exactly $\phi(d)$ elements of order equal to d. Since every element of $\mathbb{Z}_{q-1}$ has an order that divides $q - 1$, we have

$$q - 1 = \sum_{d|(q-1)} \phi(d).$$

■

We are now ready to prove our main result about multiplicative groups of finite fields.

Theorem 3.3 *Multiplicative group of a finite field*

The multiplicative group of every finite field is cyclic.

Proof Let F be a finite field of order $q = p^n$ for some prime p. We know that its multiplicative group $F^* = F\backslash\{0\}$ is abelian and has order $q-1$. We need to show that this group is, in fact, cyclic.

Firstly, for any positive divisor d of $q-1$ let a_d be the number of elements of F^* of multiplicative order equal to d. Since every element of F^* has some order and this order is a positive divisor of $q-1$, we have

$$\sum_{d|(q-1)} a_d = q-1.$$

Secondly, by Lemma 3.1 if $a_d > 0$ then $a_d = \phi(d)$.

Thirdly, by Lemma 3.2 we have $q-1 = \sum_{d|(q-1)} \phi(d)$.

These three conditions hold simultaneously only when $a_d = \phi(d)$ for every positive divisor d of $q-1$, that is, it is impossible to have $a_d = 0$ if d divides $q-1$. In particular, for $d = q-1$ we have $a_{q-1} = \phi(q-1)$. This means that the group F^*, of order $q-1$, contains an element of order equal to $q-1$ (in fact, our argument shows that F^* contains $\phi(q-1)$ such elements). But the existence of an element of order $q-1 = |F^*|$ means that the group F^* is cyclic, since such an element generates F^*. ■

In the theory of finite fields, generators of the multiplicative groups play such an important role that they have a special name.

Definition 3.4 *Primitive element*

Any generator of the multiplicative group of a finite field F is called a **primitive element** of F.

With the help of Euler's ϕ-function we are able to determine the number of primitive elements in any finite field.

Corollary 3.5

For any prime p, let F be a field of order $q = p^n$.

(a) Let ξ be a primitive element of F. Then

$$\{\xi^j : 1 \le j < q-1,\ j \text{ and } q-1 \text{ are relatively prime}\}$$

is the set of all the primitive elements of F.

(b) The number of primitive elements of a finite field of order p^n is equal to $\phi(p^n - 1)$.

Proof

(a) Since, by definition, ξ is a generator of the multiplicative group F^* of F, we have $F^* = \{1, \xi, \xi^2, \ldots, \xi^{q-2}\}$, and hence the complete list of the elements of F is $\{0, 1, \xi, \ldots, \xi^j, \ldots, \xi^{q-2}\}$. Then the map $\xi^j \mapsto j$ from the multiplicative group F^* onto the additive group $\mathbb{Z}_{q-1} = \{0, 1, \ldots, j, \ldots, q-2\}$ is an isomorphism. We know that the generators of $\mathbb{Z}_{q-1}$ are the elements j such that j and $q-1$ are relatively prime. The above isomorphism gives the required result.

(b) This follows from (a) and from the definition of $\phi(p^n - 1)$. ■

The next five exercises should help you become familiar with various aspects of calculations in finite fields.

Exercise 3.3

Let $\mathbb{Z}_3(i)$ be the extension field of $\mathbb{Z}_3$ by i where $i^2 + 1 = 0$.

(a) Write down the successive powers of $1 + i$.

(b) Find the primitive elements of the field $\mathbb{Z}_3(i)$.

Exercise 3.4

Show that 2 is a primitive element in $\mathbb{Z}_5$, $\mathbb{Z}_{11}$, $\mathbb{Z}_{13}$ and $\mathbb{Z}_{19}$.

Exercise 3.5

Show that 3 is a primitive element in $\mathbb{Z}_7$, $\mathbb{Z}_{17}$ and $\mathbb{Z}_{19}$.

Exercise 3.6

Express every non-zero element of the field $\mathbb{Z}_{11}$ in the form 2^n, $1 \leq n \leq 10$.

(a) Write down the non-zero elements of $\mathbb{Z}_{11}$ that are squares. For which values of $a \in \mathbb{Z}_{11}^*$ is the polynomial $t^2 - a$ irreducible?

(b) Write down the non-zero elements of $\mathbb{Z}_{11}$ that are cubes. For which values of $a \in \mathbb{Z}_{11}^*$ is the polynomial $t^3 - a$ irreducible?

(c) Find all primitive elements of $\mathbb{Z}_{11}$ and express them as powers of 2.

Exercise 3.7

Express every non-zero element in the field $\mathbb{Z}_{17}$ in the form 3^n, $1 \leq n \leq 16$.

(a) Write down the non-zero elements of $\mathbb{Z}_{17}$ that are squares. For which values of $a \in \mathbb{Z}_{17}^*$ is the polynomial $t^2 - a$ irreducible?

(b) Write down the non-zero elements of $\mathbb{Z}_{17}$ that are cubes. For which values of $a \in \mathbb{Z}_{17}^*$ is the polynomial $t^3 - a$ irreducible?

(c) Find all the primitive elements of $\mathbb{Z}_{17}$ and express them as powers of 3.

3.2 Roots and inverses in the multiplicative group

Primitive elements in finite fields are those of largest order in the (cyclic) multiplicative group of the field. The next definition offers a different viewpoint on the orders of the elements of the multiplicative group of a general (not necessarily finite) field.

Definition 3.6 *Roots of unity*

Let F be a field. Then any root of the polynomial $x^k - 1$ in F is known as a kth **root of unity**. Those elements $u \in F$ that have multiplicative order k in the multiplicative group F^* are called **primitive** kth roots of unity.

Since Definition 3.6 applies to arbitrary fields, you may want to know what it says about the field $\mathbb{C}$ of complex numbers that you are familiar with.

Example 3.7 *Roots of unity in $\mathbb{C}$*

If F is the field $\mathbb{C}$ of complex numbers, then the kth roots of unity are precisely the k complex numbers of the form $\cos(\frac{2\pi m}{k}) + i\sin(\frac{2\pi m}{k})$, where $0 \leq m \leq k-1$. Observe that if $\eta_k = \cos(\frac{2\pi}{k}) + i\sin(\frac{2\pi}{k})$, then, by the well-known de Moivre formula, $\eta_k^m = \cos(\frac{2\pi m}{k}) + i\sin(\frac{2\pi m}{k})$ for all m. Hence the set of all complex kth roots of unity is

$$\{\eta_k^m \ : \ 0 \leq m \leq k-1\}.$$

The set of primitive complex kth roots of unity contains all the elements η_k^m for which k and m are relatively prime. That is, there are precisely $\phi(k)$ primitive complex kth roots of unity, where $\phi(k)$ is the value of Euler's ϕ-function at k.

We now return to finite fields. The next theorem gives a simple criterion for a finite field to contain a primitive kth root of unity.

Theorem 3.8

A finite field F of order a prime power $q = p^n$ contains a primitive kth root of unity if, and only if, k is a divisor of $p^n - 1$. In this case, F contains precisely $\phi(k)$ primitive kth roots of unity.

Proof It is sufficient to note that the existence of a primitive kth root of unity in F is equivalent to the existence of an element of order equal to k in the multiplicative group, F^*, of the field. By Theorem 3.3, the multiplicative group of F is cyclic, and hence isomorphic to the additive group $(\mathbb{Z}_{q-1}, +)$. By Lagrange's Theorem, if this group contains an element of order k, then k is a divisor of $q-1$. Conversely, if k divides $q-1$, then by the result of Exercise 3.2, all elements of order exactly k in the additive group $\mathbb{Z}_{q-1} = \{0, 1, 2, \ldots, q-1\}$ have the form $j(q-1)/k$, where j and k are relatively prime. The result follows. ■

As an application of Theorem 3.8 we prove a useful observation about the existence of a square root (that is, the 2nd root) of -1 in a finite field.

Proposition 3.9

In a finite field F of order p^n, the element -1 has no square root in F if, and only if, $p \equiv 3 \pmod 4$ and n is odd.

Proof The square roots of 1 in F are ± 1 and so any primitive 4th root of unity must be a square root of -1. Hence $-1 \in F$ has a square root in F if, and only if, F has a primitive 4th root of unity.

If $p \equiv 3 \pmod 4$ and $n = 2k+1$, then $p^n = p^{2k+1} = (p^2)^k p \equiv 3 \pmod 4$, since $p^2 \equiv 1 \pmod 4$, and so $p^n - 1 \equiv 2 \pmod 4$. Thus 4 does not divide $p^n - 1$ and so, by Theorem 3.8, F does not have a primitive 4th root of unity. Thus $-1 \in F$ has no square root in F if $p \equiv 3 \pmod 4$.

Now suppose conversely that either $p \not\equiv 3 \pmod 4$ or that n is even.

Firstly, if $p = 2$, then $-1 = 1$ and so -1 has a square root in F, namely, -1 itself.

Secondly, let p be odd and let $p \equiv 1 \pmod 4$. Then $p^n \equiv 1 \pmod 4$ and so $p^n - 1$ is divisible by 4. Then by Theorem 3.8, F has a primitive 4th root of unity, which will be a square root of -1.

Finally, suppose that $p \equiv 3 \pmod 4$ and n is even. Then $p^n \equiv 1 \pmod 4$ and so $p^n - 1$ is divisible by 4. Then by Theorem 3.8, F has a primitive 4th root of unity, which will be a square root of -1. We have shown that in each case F has a square root of -1. The result follows. ■

Until this point you have only encountered finite fields of prime order p, namely, $\mathbb{Z}_p$, or GF_p in an alternative notation. The next exercise asks you to describe an infinite family of fields of order p^2.

Exercise 3.8

Let p be a prime such that $p \equiv 3 \pmod 4$. With the help of Theorem 2.19 and Proposition 3.9, construct a field of order p^2.

You have seen that for a prime p and irreducible polynomial $h(x)$ in $\mathbb{Z}_p[x]$ of degree n, the field $\mathbb{Z}_p[x]/\langle h(x)\rangle$ has order p^n. You also know that the field $\mathbb{Z}_p[x]/\langle h(x)\rangle$ can be represented in the form $\mathbb{Z}_p(\alpha)$ by adjoining a root of the polynomial $h(x)$, that is, an element α such that $h(\alpha) = 0$. This subsection concludes with two worked exercises that illustrate two techniques for finding the multiplicative inverse of a particular element expressed as a polynomial in α.

Worked Exercise 3.10

Let $K = \mathbb{Z}_3(\xi)$ where $\xi^3 = \xi + 1$ (note that the polynomial $x^3 - x - 1$ is irreducible over $\mathbb{Z}_3$, so K is a field).

(a) Find the multiplicative inverse of $2\xi + 1$ in K.

(b) Find the multiplicative inverse of $\xi^2 + 1$ in K.

Solution

(a) We will try to divide $2\xi + 1$ into $1 = \xi^3 - \xi = \xi^3 + 2\xi$ in $\mathbb{Z}_3(\xi)$ (since we are working modulo 3, we have $-2 = 1$ and $-1 = 2$).

$$
\begin{array}{rl}
 & 2\xi^2 + 2\xi \\
\hline
2\xi + 1 \;) & \xi^3 + 2\xi \\
 & \xi^3 + 2\xi^2 \\
\hline
 & \xi^2 + 2\xi \\
 & \xi^2 + 2\xi \\
\hline
\end{array}
$$

We find that

$$(2\xi + 1)(2\xi^2 + 2\xi) = \xi^3 - \xi = 1,$$

so that

$$(2\xi + 1)^{-1} = 2\xi^2 + 2\xi\,.$$

(b) In this instance a single long division will be insufficient. We illustrate a general way of finding multiplicative inverses, which is to multiply the given element, in our case $\xi^2 + 1$, by an arbitrary element of K. The latter can be written in the form $a\xi^2 + b\xi + c$ for $a, b, c \in \mathbb{Z}_3$. To simplify the result, we use $\xi^3 = \xi + 1$ and $\xi^4 = \xi^2 + \xi$:

$$
\begin{aligned}
(\xi^2 + 1)(a\xi^2 + b\xi + c) &= a\xi^4 + b\xi^3 + (a + c)\xi^2 + b\xi + c \\
&= a(\xi^2 + \xi) + b(\xi + 1) + (a + c)\xi^2 + b\xi + c \\
&= (2a + c)\xi^2 + (a + 2b)\xi + b + c.
\end{aligned}
$$

We can then determine the elements a, b, c for which

$$(2a + c)\xi^2 + (a + 2b)\xi + b + c = 1$$

by comparing coefficients. Again, we are working over $\mathbb{Z}_3$, and so to simplify things we replace -1 by 2 (and -2 by 1). This gives the system of equations:

$$
\begin{aligned}
2a + c &= 0 \\
a + 2b &= 0 \\
b + c &= 1.
\end{aligned}
$$

Subtracting the third equation from the first gives $b + a = 1$, and combining this with the second equation gives $b = 2$.

Hence $a = b = c = 2$ and the multiplicative inverse of $\xi^2 + 1$ is $2\xi^2 + 2\xi + 2$ (you can check this by multiplying out $(\xi^2 + 1)(2\xi^2 + 2\xi + 2)$).

Worked Exercise 3.11

Find the multiplicative inverse of the following elements in $K = \mathbb{Z}_3(\xi)$ where $\xi^3 = \xi + 1$.

(a) ξ

(b) $\xi + 1$

(c) $\xi^2 + 2\xi + 1$

Solution

(a) We have $1 = \xi^3 - \xi = \xi(\xi^2 - 1)$ in $\mathbb{Z}_3(\xi)$, which implies that $\xi^{-1} = \xi^2 + 2$ as $-1 \equiv 2 \pmod 3$. (If you used long division or compared coefficients you will have got the same answer but with rather more work.)

(b) We divide $\xi + 1$ into $1 = \xi^3 - \xi = \xi^3 + 2\xi$ in $\mathbb{Z}_3(\xi)$.

$$\begin{array}{rl} & \xi^2 + 2\xi \\ \xi + 1 \;) & \xi^3 \quad + \quad + 2\xi \\ & \xi^3 + \xi^2 \\ \hline & \quad 2\xi^2 + 2\xi \\ & \quad 2\xi^2 + 2\xi \\ \hline \end{array}$$

and find that $(\xi + 1)^{-1} = \xi^2 + 2\xi$.

(c) In this instance one long division is again insufficient and we use the more general method. Since every element of K can be written in the form $a\xi^2 + b\xi + c$ with $a, b, c \in K$, we write

$$\begin{aligned} 1 &= (\xi^2 + 2\xi + 1)(a\xi^2 + b\xi + c) \\ &= a\xi^4 + (2a + b)\xi^3 + (a + 2b + c)\xi^2 + (b + 2c)\xi + c \\ &= a(\xi^2 + \xi) + (2a + b)(\xi + 1) + (a + 2b + c)\xi^2 + (b + 2c)\xi + c \\ &= (2a + 2b + c)\xi^2 + (2b + 2c)\xi + 2a + b + c, \end{aligned}$$

where we used $\xi^3 = \xi + 1$ and $\xi^4 = \xi^2 + \xi$ to simplify the result.

Comparing coefficients in the resulting equation

$$(2a + 2b + c)\xi^2 + (2b + 2c)\xi + 2a + b + c = 1$$

over $\mathbb{Z}_3$ leaves us with the linear system

$$\begin{aligned} 2a + 2b + c &= 0 \\ 2b + 2c &= 0 \\ 2a + b + c &= 1. \end{aligned}$$

Subtracting the third equation from the first gives $b = 2$, and substituting this in the second equation gives $4 + 2c = 0$ and hence $c = 1$. A further substitution in the first equation then gives $2a + 4 + 1 = 0$, so that $a = 2$.

Hence $a = 2$, $b = 2$, $c = 1$, and so the multiplicative inverse of $\xi^2 + 2\xi + 1$ is $2\xi^2 + 2\xi + 1$.

4 Splitting fields

The theory of field extensions originated in the hunt for solutions to polynomial equations. It is therefore reasonable to consider extensions which contain *all* the roots of a given polynomial. This section begins with a formal definition of extensions of these kind, and then shows that for a given polynomial over a field such an extension always exists and is unique up to isomorphism.

4.1 Existence and uniqueness of splitting fields

Definition 4.1 *Splitting field*

Let $f(x)$ be a polynomial of positive degree over a field F. A **splitting field** of $f(x)$ over F is a field E that has the following properties:

(a) E is an extension of F that contains all the roots of $f(x)$

(b) if L is an extension of F that contains all the roots of $f(x)$, then E is isomorphic to a subfield of L.

Definition 4.1(b) is essentially saying that E is the smallest field that contains all the roots of the polynomial.

We first prove that for a given polynomial of positive degree over a field F, there is indeed a field extension of E that contains all the roots of F.

Theorem 4.2

Let $f(x)$ be a polynomial of positive degree over a field F. Then there exists an extension of F that contains all the roots of $f(x)$.

Proof We prove this result by induction on the degree of $f(x)$.

If $f(x)$ has degree one, then $f(x)$ has its (unique) root in F.

Now suppose that the result holds for all polynomials of degree less than k for $k \geq 1$, and suppose that $f(x)$ is a polynomial of degree k.

Let $f(x) = f_1(x)f_2(x)\cdots f_m(x)$ be a factorisation into irreducible factors over F (the value $m = 1$ corresponds to the case when $f(x)$ itself is irreducible). Set $h(x) = f_1(x)$. By Corollary 2.20, $h(x)$, and hence $f(x)$, has a root in the extension $F_1 = F[x]/\langle h(x)\rangle$ of F.

Let $x_1, x_2, \ldots, x_\ell$ be the collection of all the roots of $f(x)$ that are contained in F_1; we know that this collection has at least one member. Over F_1 we then have

$$f(x) = (x - x_1)(x - x_2)\cdots(x - x_\ell)g(x),$$

where the degree of $g(x)$ is smaller than the degree of $f(x)$. By the induction hypothesis, the polynomial $g(x)$ has all its roots in some extension F_2 of F_1. But then, all the roots of $f(x)$ lie in F_2 and this is also an extension of F. ■

Definition 4.3 *Splitting polynomial*

Let F be a field. We say that a polynomial $f(x) \in F[x]$ **splits** over F if all roots of $f(x)$ lie in F.

In your previous studies, you might have met the Fundamental Theorem of Algebra, which states that any non-constant polynomial in $\mathbb{C}[x]$ has at least one root in $\mathbb{C}$. One way of phrasing this pivotal result is to say that every polynomial in $\mathbb{C}[x]$ splits over $\mathbb{C}$.

For the formulation of our next result, let us recall Definition 2.12: if F is an extension of a field K and $\alpha_1, \alpha_2, \ldots, \alpha_d \in F$, the symbol $K(\alpha_1, \ldots, \alpha_d)$ denotes the smallest subfield of F that contains K and all the elements $\alpha_1, \alpha_2, \ldots, \alpha_d$.

Proposition 4.4

Suppose that $f(x)$ is a polynomial in $K[x]$ for some field K and

1. $f(x)$ splits over an extension F of K
2. $\{\alpha_1, \alpha_2, \ldots, \alpha_d\}$ is the set of all roots of $f(x)$.

Then $K(\alpha_1, \ldots, \alpha_d)$ is a splitting field for $f(x)$ over K and $K(\alpha_1, \ldots, \alpha_d) \subseteq F$.

It may or may not be true that $K(\alpha_1, \ldots, \alpha_d) = F$.

Proof Since $f(x)$ splits over the field F, we have $\{\alpha_1, \alpha_2, \ldots, \alpha_d\} \subseteq F$, and so $K(\alpha_1, \ldots, \alpha_d)$ is a subfield of F. Since $K(\alpha_1, \ldots, \alpha_d)$ is the smallest subfield of F containing K and all the roots of $f(x)$, it is a splitting field for $f(x)$. ■

We may now state and prove the following consequence of our considerations.

Corollary 4.5 *Existence of splitting fields*

Let $f(x)$ be a polynomial of positive degree over a field F. Then there exists a splitting field of $f(x)$ over F.

Proof By Theorem 4.2, there exists an extension of F over which $f(x)$ splits. The result then follows by Proposition 4.4. ■

The next theorem shows that a splitting field for a given polynomial is unique up to isomorphism.

Theorem 4.6 *Uniqueness of splitting fields*

Let $\theta : K \to L$ be an isomorphism of fields and let $\hat{\theta} : K[x] \to L[x]$ be the extension of θ to the polynomial ring $K[x]$ defined by

$$\hat{\theta}(a_0 + a_1x + \cdots + a_nx^n) = \theta(a_0) + \theta(a_1)x + \cdots + \theta(a_n)x^n.$$

Let $f(x) \in K[x]$ have degree $d \geq 1$ and let $g(x) = \hat{\theta}(f(x))$ be its image over L. Let K_S, L_S be fields over which $f(x)$ and $g(x)$, respectively, split. Further, let $A = \{\alpha_1, \alpha_2, \ldots, \alpha_d\}$ be the set of all the roots of $f(x)$ in K_S and let $B = \{\beta_1, \beta_2, \ldots, \beta_d\}$ be the set of all the roots of $g(x)$ in L_S.

Then there is an isomorphism $\phi : K(\alpha_1, \ldots, \alpha_d) \to L(\beta_1, \ldots, \beta_d)$ such that

(a) the restriction $\phi_A : A \to B$ of ϕ to A is a bijection

(b) $\phi(k) = \theta(k)$ for every $k \in K$.

Proof We will prove the result by induction on d, the degree of the polynomial $f(x)$.

If $\deg(f) = 1$ then the polynomials $f(x)$ and $g(x)$ split over K and L, respectively, and the result is immediate from the isomorphism of K and L.

Let the degree of $f(x)$ be d for $d > 1$, and suppose that the result holds for all instances where the degree of the polynomials involved is smaller than d.

Let $f_1(x)$ be an irreducible factor of $f(x)$ over K and let $g_1(x) = \hat{\theta}(f_1(x))$ be the corresponding irreducible factor of $g(x)$ over L. We may assume without loss of generality that α_1 is a root of $f_1(x)$ and β_1 is a root of $g_1(x)$.

By Theorem 2.28, there is an isomorphism θ_1 from the field $K_1 = K(\alpha_1)$ onto the field $L_1 = L(\beta_1)$ such that $\theta_1(\alpha_1) = \beta_1$ and $\theta_1(k) = \theta(k)$ for all $k \in K$.

Since α_1 and β_1 are roots of $f(x)$ and $g(x)$ in the fields K_1 and L_1, the two polynomials factor as $f(x) = (x - \alpha_1)f_2(x)$ and $g(x) = (x - \beta_1)g_2(x)$, where $f_2(x)$ and $g_2(x)$ are polynomials over K_1 and L_1, respectively.

Let $\hat{\theta}_1$ be the extension of θ to $K_1[x]$. Then

$$\hat{\theta}_1(f(x)) = (x - \theta_1(\alpha_1))\hat{\theta}_1(f_2(x)), \text{ that is, } \hat{\theta}_1(f(x)) = (x - \beta_1)\hat{\theta}_1(f_2(x))$$

over the field $L_1 = \theta_1(K_1)$. But the coefficients in $f(x)$ on the left-hand side of this equation all lie in K. Hence $\hat{\theta}_1(f(x)) = \hat{\theta}(f(x)) = g(x)$, and therefore $g(x) = (x - \beta_1)\hat{\theta}_1(f_2(x))$.

Recall also that $g(x) = (x - \beta_1)g_2(x)$ for some polynomial $g_2(x)$ over L_1. Comparing the last two equations gives $g_2(x) = \hat{\theta}_1(f_2(x))$ since $L_1[x]$ is a unique factorisation domain (see Book C, Chapter 11, Theorem 3.1).

Hence $K_1(\alpha_2, \ldots, \alpha_d)$ is the splitting field of $f_2(x)$ over K_1, while $L_1(\beta_2, \ldots, \beta_d)$ is the splitting field of $g_2(x)$ over L_1. In addition, $\theta_1 : K_1 \to L_1$ is a field isomorphism such that $\hat{\theta}_1(f_2(x)) = g_2(x)$.

Since the degree of $f_1(x)$ is smaller than d, we may apply the induction hypothesis. That is, we may assume the existence of a field isomorphism $\phi : K_1(\alpha_2, \ldots, \alpha_d) \to L_1(\beta_2, \ldots, \beta_d)$ such that ϕ maps the set $\{\alpha_2, \ldots, \alpha_d\}$ onto the set $\{\beta_2, \ldots, \beta_d\}$, and $\phi(z) = \theta_1(z)$ for all $z \in K_1$.

However, we saw above that $\theta_1(\alpha_1) = \beta_1$ and $\theta_1(k) = \theta(k)$ for each $k \in K$. This implies that $\phi(\alpha_1) = \beta_1$ and $\phi(k) = \theta(k)$ for all $k \in K$. In other words, ϕ is also an isomorphism from the field $K(\alpha_1, \alpha_2, \ldots, \alpha_d)$ onto the field $L(\beta_1, \beta_2, \ldots, \beta_d)$ with the required properties. The result now follows by induction. ■

The next corollary gives a more descriptive statement of Theorem 4.6.

Corollary 4.7

Let $f(x)$ be a polynomial over a field F. Then all splitting fields for $f(x)$ are mutually isomorphic.

The next two worked exercises invite you to practise with splitting fields for quadratic polynomials, that is, polynomials of degree 2.

Worked Exercise 4.8

Show that if $h(x)$ is an irreducible quadratic polynomial in $F[x]$, then $E = F[x]/\langle h(x)\rangle$ is a splitting field for $h(x)$ over F.

Hint: show that $h(x)$ factorises into linear factors in $E[x]$.

Solution

Elements of $F[x]/\langle h(x)\rangle$ have the form $a + b\alpha$ where $h(\alpha) = 0$, so that multiplication is carried out modulo $h(\alpha)$. Consider the polynomial ring $E[x]$ and the polynomial $h(x) \in E[x]$.

As $h(\alpha) = 0$, the remainder on dividing $h(x)$ by $x - \alpha$ is zero, that is, $h(x) = (x - \alpha)g(x)$ in $E[x]$. Now, $h(x)$ is a quadratic polynomial, and so $g(x)$ is linear and has a root $\beta \in E$. Thus both roots of $h(x)$ are in E and so E contains a splitting field for $h(x)$. Since any splitting field for $h(x)$ must contain F and α, and $F[x]/\langle h(x)\rangle \cong F(\alpha)$, $F(\alpha)$ is a splitting field for $h(x)$.

Worked Exercise 4.9

(a) Let F be a field. Show that for any non-zero $a \in F$, $x^2 + ax + a^2$ is irreducible in $F[x]$ if, and only if, $x^2 + x + 1$ is irreducible in $F[x]$.

(b) Let F be a field and let $a \in F$ with $a \neq 0$. Show that if $x^2 + x + 1$ is irreducible in F, then $F[x]/\langle x^2 + x + 1\rangle$ is a splitting field for $x^2 + ax + a^2$ over F.

Solution

(a) Suppose that $x^2 + x + 1$ is reducible in $F[x]$, so that there is $b \in F$ such that $b^2 + b + 1 = 0$. Then $x^2 + ax + a^2 = (x - ab)(x - ab^2)$, and so $x^2 + ax + a^2$ is reducible in $F[x]$.

Now suppose that $x^2 + ax + a^2$ is reducible in $F[x]$ so that there is a $c \in F$ with $c^2 + ac + a^2 = 0$. Letting $b = ca^{-1} \in F$ gives

$$\begin{aligned} b^2 + b + 1 &= (ca^{-1})^2 + ca^{-1} + 1 \\ &= c^2(a^{-1})^2 + ca(a^{-1})^2 + a^2(a^{-1})^2 \\ &= (c^2 + ac + a^2)(a^{-1})^2 = 0, \end{aligned}$$

so that b is a root of $x^2 + x + 1$ and $x^2 + x + 1$ is reducible in $F[x]$.

(b) By Theorem 2.19, we know that $F[x]/\langle x^2 + x + 1\rangle \cong F(\alpha)$, where α is such that $\alpha^2 + \alpha + 1 = 0$. The elements of $F(\alpha)$ have the form $u + v\alpha$ where $u, v \in F$, and $x^2 + x + 1$ is reducible in $F(\alpha)[x]$. Then, by part (a), $x^2 + ax + a^2$ is reducible in $F(\alpha)[x]$, and so $F(\alpha)$ contains a splitting field for $x^2 + ax + a^2$ over F.

Since $x^2 + x + 1$ is irreducible in $F[x]$, by part (a) $x^2 + ax + a^2$ is irreducible in $F[x]$, and so F is not a splitting field for $x^2 + ax + a^2$. As $[F(\alpha) : F] = 2$, there is no extension E of F with $F \subset E \subset F(\alpha)$, and so $F(\alpha) \cong F[x]/\langle x^2 + x + 1\rangle$ is a splitting field for $x^2 + ax + a^2$ over F.

After practising with quadratic polynomials, you may now wish to see a calculation of a splitting field for a cubic polynomial.

Example 4.10 *A splitting field for $x^3 - 2$ over $\mathbb{Q}$*

We are going to find a splitting field for $x^3 - 2$ over $\mathbb{Q}$. In Example 2.26 we found three extensions of $\mathbb{Q}$ isomorphic to $\mathbb{Q}[x]/\langle x^3 - 2\rangle$, one corresponding to each root of $x^3 - 2$ in $\mathbb{C}$.

Let $L = \mathbb{Q}(\sqrt[3]{2})$. We know that L is not a splitting field for $x^3 - 2$ since it does not contain the root $\omega\sqrt[3]{2}$, where $\omega = e^{\frac{2i\pi}{3}}$, as $L \subseteq \mathbb{R}$ and $\omega\sqrt[3]{2} \notin \mathbb{R}$.

Since we know that $\sqrt[3]{2}$ is a root of $x^3 - 2$ in $L[x]$, we can factorise this polynomial in $L[x]$ to obtain

$$x^3 - 2 = (x - \sqrt[3]{2})(x^2 + \sqrt[3]{2}x + \sqrt[3]{2}^2).$$

Since $L = \mathbb{Q}(\sqrt[3]{2})$ is not a splitting field for $x^3 - 2$ over $\mathbb{Q}$, the quadratic $x^2 + \sqrt[3]{2}x + \sqrt[3]{2}^2$ must be irreducible in $L[x]$ since otherwise it must factor into two linear factors, and this implies that both roots of the polynomial are in L.

By the solution to Worked Exercise 4.9, a splitting field over L for $x^2 + x + 1$ is also a splitting field for $x^2 + \sqrt[3]{2}x + \sqrt[3]{2}^2$. It is therefore sufficient to consider the extension $L(\omega) \cong L[x]/\langle h(x)\rangle$ where $h(x) = x^2 + x + 1$ and ω is a root of $h(x)$.

Now as $h(\omega) = 0$, $h(x)$ is not irreducible in $L(\omega)[x]$. Hence by the solution to Worked Exercise 4.8, $L(\omega)$ is a splitting field for $h(x)$ over L. It is clear that $x^3 - 2$ splits over $L(\omega)$. We need to show that there is no field smaller than $L(\omega)$ over which $x^3 - 2$ splits.

We know that the elements of $L(\omega)$ can be written as $a + b\omega$ for $a, b \in L$ and the elements of L can be written as $r + s\alpha + t\alpha^2$ for $r, s, t \in \mathbb{Q}$ and $\alpha = \sqrt[3]{2}$. Thus, the elements of $L(\omega)$ can be written in the form

$$r + s\alpha + t\alpha^2 + (r_1 + s_1\alpha + t_1\alpha^2)\omega = r + s\alpha + t\alpha^2 + r_1\omega + s_1\alpha\omega + t_1\alpha^2\omega$$

where $r, s, t, r_1, s_1, t_1 \in \mathbb{Q}$.

Since α and $\alpha\omega$ must both be in a splitting field, ω must be in a splitting field, and since $\omega \notin L$, no field smaller than $L(\omega)$ can contain all these elements. Hence a splitting field for $x^3 - 2$ is $L(\omega) = \mathbb{Q}(\sqrt[3]{2})(\omega)$.

Note that by Theorem 2.29, the field $L(\omega) = \mathbb{Q}(\sqrt[3]{2})(\omega)$ is an extension of degree 6 over $\mathbb{Q}$. Equivalently, $L(\omega)$ is a vector space of dimension 6 over $\mathbb{Q}$.

In Example 4.10, we made considerable use of our knowledge of $\mathbb{C}$. Since the Fundamental Theorem of Algebra tells us that every non-constant polynomial over $\mathbb{C}$ factorises completely into linear factors, we know that any splitting field for a polynomial in $\mathbb{Q}[x]$ will be contained in $\mathbb{C}$ and will contain the roots of the polynomial. We may therefore refer to 'the' splitting field of a polynomial over $\mathbb{Q}$.

The crucial step in Example 4.10 was to observe that $x^2 + \sqrt[3]{2}x + \sqrt[3]{2}^2$ is an irreducible polynomial over $L[x]$. The next example shows that this is not always the case in other fields.

Example 4.11 *A splitting field for $x^3 - 2$ over $\mathbb{Z}_{13}$*

Consider the polynomial $x^3 - 2 \in \mathbb{Z}_{13}[x]$. If a cubic polynomial is reducible over a field, it must have a linear factor and hence a root in that field. By inspection, we find that only $1, 5, 8, 12$ occur as cubes in $\mathbb{Z}_{13}$, and so $x^3 - 2$ is irreducible over $\mathbb{Z}_{13}$ since it has no root in $\mathbb{Z}_{13}$.

In order to determine the splitting field of $x^3 - 2$, we begin by forming the extension field $L = \mathbb{Z}_{13}[x]/\langle h(x)\rangle$, as in Example 4.10, and note that the elements of this field can be written in the form $r + s\alpha + t\alpha^2$ where $r, s, t \in \mathbb{Z}_{13}$ and $h(\alpha) = 0$, so that $\alpha^3 = 2$.

As before, $x^3 - 2 = (x - \alpha)(x^2 + \alpha x + \alpha^2)$, so we can refer to the solution of Worked Exercise 4.9 and note that $x^2 + \alpha x + \alpha^2$ is irreducible in $L[x]$ if, and only if, $x^2 + x + 1$ is irreducible in $L[x]$.

Since $x^3 - 1 = (x - 1)(x^2 + x + 1)$, the polynomial $x^2 + x + 1$ is reducible in $\mathbb{Z}_{13}[x]$ if, and only if, $\mathbb{Z}_{13}$ contains a primitive cube root of unity. Since $3^3 \equiv 1 \pmod{13}$, the field $\mathbb{Z}_{13}$ does contain a primitive cube root of unity, and so $x^2 + x + 1$ is reducible in $\mathbb{Z}_{13}[x]$. In fact, one may check that

$$x^2 + x + 1 = (x - 3)(x - 9) = (x + 10)(x + 4)$$

in $\mathbb{Z}_{13}[x]$, and so the polynomial is reducible in $L[x]$. Hence $x^2 + \alpha x + \alpha^2$ is reducible in $L[x]$ and so L contains a splitting field for $x^3 - 2$. Since any splitting field must contain α, the field L is a splitting field for $x^3 - 2$.

As an aside, note that the field $\mathbb{Z}_{13}(\sqrt[3]{2})$ has 13^3 elements. In the solution to Exercise 3.8 you saw a construction of a field with p^2 elements for any prime p such that $p \equiv 3 \pmod{4}$, and in Worked Exercise 1.8 you saw a field with 13^2 elements. This raises the natural question of what the number of elements of a finite field can be. We address this question in the next subsection and conclude with an exercise about splitting fields of cubic polynomials over finite fields.

Exercise 4.1

Find a splitting field for $x^3 - 2$ over

(a) $\mathbb{Z}_3$

(b) $\mathbb{Z}_5$.

4.2 Existence and uniqueness of finite fields

When we observed that we could regard a field extension as a vector space over the base field, we showed as a consequence that every finite field has order p^n for some n. In this last subsection of the chapter we will prove that not only does a field of order p^n exist for all primes p and all positive integers n but any two finite fields of the same order are isomorphic. This gives a classification of finite fields.

The approach to finding a field of order p^n is to find a polynomial of degree n and a field over which the polynomial splits. We then show that this field has order p^n.

Theorem 4.12

Let F be a finite field of order $q = p^n$ for some prime p. Then every element of F is a root of the polynomial $x^q - x$.

Proof The element $0 \in F$ is clearly a root of $x^q - x = x(x^{q-1} - 1)$. Thus, we only need to prove that any non-zero element of F is a root of the polynomial $x^{q-1} - 1$. As we know, the multiplicative group of F has order $q - 1$. By Lagrange's Theorem, the order of any element of a group is a divisor of the order of the group. Therefore for every x in the multiplicative group F^* $(= F\backslash\{0\})$ of the field F we have $x^{q-1} = 1$. Equivalently, every non-zero element of F is a root of $x^{q-1} - 1$. We conclude that every element of F is a root of the polynomial $x^q - x$. ■

We will gradually add more details to our setting for proving that for a given prime number p and any positive integer n there is a field of order p^n. As mentioned earlier, we will do this by constructing a splitting field of a specific polynomial over $\mathbb{Z}_p$. At some stage of the proof we will need to show that a certain polynomial has no repeated roots. We will do so by making use of an analogue of differentiation in a polynomial ring over a general field.

Definition 4.13 *Formal derivative*

Let K be a field. Let the mapping $d : K[x] \to K[x]$ be defined by

$$d(a_0 + a_1x + a_2x^2 + \cdots + a_nx^n) = a_1 + 2a_2x + \cdots + na_nx^{n-1}.$$

We call the map d the **formal derivative**.

For polynomials over $\mathbb{R}$ or $\mathbb{C}$, the formal derivative is just the standard derivative.

The next lemma shows that the formal derivative behaves like the familiar derivative in real analysis as regards sums and products of polynomials.

Lemma 4.14

Let K be a field and let $d : K[x] \to K[x]$ be the formal derivative. Then, for any two polynomials $f(x), g(x) \in K[x]$, we have

(a) $d(f(x) + g(x)) = d(f(x)) + d(g(x))$

(b) $d(f(x)g(x)) = d(f(x))g(x) + f(x)d(g(x))$.

Proof

(a) Let $f(x) = a_0 + a_1x + \cdots + a_nx^n$ and $g(x) = b_0 + b_1x + \cdots + b_nx^n$. Then $f(x) + g(x) = a_0 + b_0 + (a_1 + b_1)x + \cdots + (a_n + b_n)x^n$, and

$$\begin{aligned} d(f(x) + g(x)) &= d(a_0 + b_0 + (a_1 + b_1)x + \cdots + (a_n + b_n)x^n) \\ &= a_1 + b_1 + 2(a_2 + b_2)x + \cdots + n(a_n + b_n)x^{n-1} \\ &= a_1 + 2a_2x + \cdots + na_nx^{n-1} + b_1 + 2b_2x + \cdots + ba_nx^{n-1} \\ &= d(f(x)) + d(g(x)). \end{aligned}$$

(b) We prove the result in the special case $f(x) = ax^j$ and $g(x) = bx^k$. The general result then follows by part (a). We have

$$\begin{aligned} d(ax^jbx^k) &= d(abx^{j+k}) \\ &= (j + k)abx^{j+k-1} \\ &= jabx^{j+k-1} + kabx^{j+k-1} \\ &= jax^{j-1}bx^k + ax^j(kbx^{k-1}) \\ &= d(f(x))g(x) + f(x)d(g(x)). \end{aligned}$$

■

The formal derivative of Definition 4.13 is not the only map with properties (a) and (b) in Lemma 4.14; for example, the mapping $d_1 : K[x] \to K[x]$ defined by $d_1(f(x)) = xd(f(x))$ also satisfies them. A map that satisfy these two properties is called a **derivation** and it is a generalisation of the familiar operation of differentiation.

We are now ready to prove a lemma about the formal derivative that is an analogue of the familiar result from elementary calculus that a polynomial has a repeated root if, and only if, its derivative also has that root.

Lemma 4.15

Let K be a field and let $f(x)$ be a non-zero polynomial in $K[x]$. Let F be the splitting field for $f(x)$ over K. Then $f(x)$ has a root $\alpha \in F$ of multiplicity $m \geq 2$ if, and only if, the highest common factor of $f(x)$ and its formal derivative $d(f(x))$ is a polynomial of positive degree.

Proof Suppose that $\alpha \in F$ is a root of $f(x)$ of multiplicity $m \geq 2$. This is equivalent to saying that $f(x) = (x - \alpha)^m g(x)$ for some $g(x) \in F[x]$ and some $m \geq 2$.

The formal derivative d of $f(x)$ is given by

$$\begin{aligned} d(x^q - x) &= d((x-\alpha)^m g(x)) \\ &= m(x-\alpha)^{m-1} g(x) + (x-\alpha)^m d(g(x)) \\ &= (x-\alpha)^{m-1}[mg(x) + (x-\alpha)d(g(x))] \\ &= (x-\alpha)h(x), \end{aligned}$$

where $h(x) = (x-\alpha)^{m-2}[mg(x) + (x-\alpha)d(g(x))]$ is a (possibly constant) polynomial, since $m \geq 2$.

Thus the highest common factor of $f(x)$ and $d(f(x))$ is a multiple of $x - \alpha$, and so a polynomial of positive degree.

Now suppose that $f(x)$ and $d(f(x))$ are both multiples of a polynomial $h(x)$ that has positive degree. Then $h(x)$ has a root α in the splitting field F and so $f(x)$ and $d(f(x))$ are both multiples of $x - \alpha$. Let $f(x) = (x-\alpha)g(x)$. Then

$$\begin{aligned} d(f(x)) &= d((x-\alpha)g(x)) \\ &= (x-\alpha)d(g(x)) + g(x) \text{ by Lemma 4.14.} \end{aligned}$$

Since $d(f(x))$ is a multiple of $x - \alpha$, this implies that $g(x) = (x-\alpha)k(x)$ for some $k(x) \in F[x]$ and so $f(x) = (x-\alpha)^2 k(x)$. Thus $f(x)$ has a multiple root in the splitting field F. ■

We use this lemma to show that a particular polynomial has no repeated roots.

Lemma 4.16

Let $q = p^n$ be a prime power, let $f(x) = x^q - x \in \mathbb{Z}_p[x]$, and let F be a splitting field for $f(x)$ over $\mathbb{Z}_p$. Then the polynomial $f(x)$ has no repeated roots in F.

Proof By Corollary 4.5, there exists a splitting field for $f(x)$ over $\mathbb{Z}_p$. That is, there exists a field F containing $\mathbb{Z}_p$ such that every root of $f(x)$ lies in F, and (up to isomorphism) F is the smallest field with this property. Note that the characteristic of F is p since it contains $\mathbb{Z}_p$.

Suppose that $\alpha \in F$ is a root of $f(x)$ of multiplicity $m \geq 2$. Then, by Lemma 4.15, $d(f(x))$ is a multiple of $x - \alpha$, that is, $d(f(x)) = (x-\alpha)h(x)$ for some $h(x) \in F[x]$.

But $d(x^q - x) = qx^{q-1} - 1 = -1$ since $q \equiv 0 \pmod{p}$, which implies that $-1 = (x-\alpha)h(x)$. But this is absurd in $F[x]$. This contradiction shows that all roots of $f(x) = x^q - x$ in its splitting field F are distinct. ■

The next theorem is a significant result. It classifies all finite fields, and it is the aim we have been working towards with our discussion of splitting fields. A key step in the proof is to show that the splitting field of the polynomial $x^q - x$ for $q = p^n$ has order p^n.

Theorem 4.17 *Classification of finite fields*

For every prime p and every $n \geq 1$ there exists a field of order p^n, and any two fields of order p^n are isomorphic.

Proof *Existence* Let p and n be as in the statement, and let $q = p^n$. Consider the polynomial $f(x) = x^q - x$ over $\mathbb{Z}_p$. By Lemma 4.16 there exists a splitting field F for $f(x)$ over $\mathbb{Z}_p$ and $f(x)$ has no repeated roots in F.

Let A be the set of all the roots of $f(x)$ in the field F. Since the degree of $f(x)$ is q, the roots of $f(x)$ are mutually distinct, and since by the proof of Proposition 4.3 of Book C, Chapter 11, a polynomial of degree q with all roots distinct has exactly q roots in F, it follows that $|A| = q = p^n$. We would like to prove a perhaps unexpected fact – namely, that A is a subfield of F.

Firstly note that if $u \in A$ with $u \neq 0$ then $u^q - u = 0$ and so (using $\frac{1}{u}$ for u^{-1} for ease of reading) $\left(\frac{1}{u}\right)^q - \frac{1}{u} = \frac{u - u^q}{u^{q+1}} = 0$ and so $u^{-1} \in A$. Thus, to show that A is a subfield it is sufficient to convince ourselves that for any two elements $u, v \in A$ we have $u + v \in A$ and $uv \in A$; note that 0 and 1 belong to A since both are roots of $f(x)$.

Let $u, v \in A$, that is, $u^q - u = 0$ and $v^q - v = 0$, or, equivalently, $u^q = u$ and $v^q = v$. By Theorem 1.12 we have $(u + v)^q = u^q + v^q = u + v$. This means if u and v are roots of $f(x)$, then so is the element $u + v$. In other words, if $u, v \in A$, then $u + v \in A$. Moreover, $(uv)^q = u^q v^q = uv$. This shows that if $u, v \in A$, then $uv \in A$. It follows that A is a field, as claimed.

But since $A \subseteq F$ and F was assumed to be the smallest field containing all the roots of $f(x)$, we have $A = F$. As $|A| = |F| = q = p^n$, we have proved the existence of a field of order p^n.

Isomorphism Let K be a field of order $q = p^n$, and hence of characteristic p. By Theorem 1.11 we may assume that the field $\mathbb{Z}_p$ is a subfield of K. In the proof of Theorem 4.12 we saw that every element of K is a root of the polynomial $f(x) = x^q - x$ over $\mathbb{Z}_p$. Since this polynomial cannot have more than q roots, it follows that K is a splitting field for $f(x)$ over $\mathbb{Z}_p$.

Corollary 4.7 asserts that any two splitting fields of a polynomial over $\mathbb{Z}_p$ are isomorphic. It follows that any two finite fields of the same order are isomorphic. ■

Now that we know that a field of order p^n exists for every prime power, we show how to construct an irreducible polynomial of degree n over $\mathbb{Z}_p$.

Corollary 4.18

For any prime p and any positive integer n there exists an irreducible polynomial of degree n over $\mathbb{Z}_p$.

Proof By Theorem 4.17 there exists a field F of order p^n that contains $\mathbb{Z}_p$ as a subfield. Let ξ be a primitive element of F, that is an element that generates the multiplicative group $F\backslash\{0\}$.

Let us regard the field F as a vector space over $\mathbb{Z}_p$. The $n+1$ elements $1, \xi, \xi^2, \ldots, \xi^n$ must be linearly dependent, since the degree of F over $\mathbb{Z}_p$ is equal to n. It follows that there exist elements $a_0, a_1, \ldots, a_{n-1}, a_n \in \mathbb{Z}_p$ such that $a_0 1 + a_1\xi + \cdots + a_{n-1}\xi^{n-1} + a_n\xi^n = 0$. This means that ξ is a root of the polynomial $f(x) = a_0 + a_1 x + \cdots + a_{n-1}x^{n-1} + a_n x^n$ over $\mathbb{Z}_p$. We now show that $f(x)$ is irreducible and of degree n.

Suppose the contrary, that is, suppose that either $f(x)$ has degree smaller than n, or $f(x)$ is reducible over $\mathbb{Z}_p$. In either case we may assume that $f(x)$ has an irreducible divisor $h(x) \in \mathbb{Z}_p[x]$ of degree d, where $1 \leq d \leq n-1$, such that ξ is a root of $h(x)$.

Consider the field $E = \mathbb{Z}_p(\xi)$, that is, the smallest subfield of F containing $\mathbb{Z}_p$ and the element ξ. Since ξ is a root of an irreducible polynomial $h(x) \in \mathbb{Z}_p$ of degree $d < n$, by Proposition 2.19 all the elements of the field E have the form $b_0 + b_1\xi + \cdots + b_{d-1}\xi^{d-1}$, where $b_0, b_1, \ldots, b_{d-1} \in \mathbb{Z}_p$.

Since E has order p^d and contains the element ξ, the multiplicative order of ξ in E must be a divisor of $p^d - 1$. But E is a subfield of F and the orders of ξ in both these fields are the same. This contradicts our assumption that ξ is a primitive element, that is, an element of order $p^n - 1$, in F.

It follows that $f(x)$ is an irreducible polynomial of degree n over $\mathbb{Z}_p$, which completes the proof. ■

In the next worked exercise we will construct an irreducible polynomial of degree 2 over $\mathbb{Z}_3$ using the method outlined in the above proof. Of course, for degree 2 you would be able to find such a polynomial by other means, but finding one using the theorem in a simple case makes it easier to approach harder cases.

Worked Exercise 4.19

Use the approach given in the proof of Corollary 4.18 to find an irreducible polynomial of degree 2 over $\mathbb{Z}_3$.

Solution

The first step is to find a primitive element in the field of order 9. In order to do this we need to have a way of writing down the elements of the field. We use the solution to Exercise 3.3 where we found the primitive elements of the field $\mathbb{Z}_3[x]/\langle x^2+1\rangle = \{a + bi : a, b \in \mathbb{Z}_3\}$. (Yes, x^2+1 is irreducible over $\mathbb{Z}_3[x]$, but we will find another irreducible polynomial.) From Exercise 3.3 we know that $1 + i$ is a primitive element in this field.

The next step is to find $a, b, c \in \mathbb{Z}_3$, not all zero, such that

$$a + b(1 + i) + c(1 + i)^2 = 0$$

(a key point in the proof of Corollary 4.18 is that such a, b, c do exist). Since $i^2 = -1 = 2$ in $\mathbb{Z}_3$, this equation is equivalent to

$$(a + b) + (b + 2c)i = 0,$$

and, since 1 and i are linearly independent over $\mathbb{Z}_3$, it follows that $a + b = 0$ and $b + 2c = 0 \pmod 3$. This is a homogeneous linear system consisting of two equations and three unknowns and so there will be more than one solution. We, however, just need one (non-zero) solution. Letting, for example, $b = 1$ gives $c = 1$ and $a = 2$.

Thus, another example of an irreducible polynomial of degree 2 in $\mathbb{Z}_3[x]$ is $2 + x + x^2$.

This subsection, and this chapter, end with a worked exercise in which you are invited to follow the construction of an irreducible polynomial of degree 4 over $\mathbb{Z}_2$.

Worked Exercise 4.20

(a) Suppose that $\mathbb{Z}_2(\omega) \cong \mathbb{Z}_2[x]/\langle x^2 + x + 1\rangle$. Show that the polynomial $f(x) = x^2 + x + \omega$ is irreducible in $\mathbb{Z}_2(\omega)[x]$.

(b) Let $\mathbb{Z}_2(\omega, \alpha)$ be an extension of the field $\mathbb{Z}_2$ isomorphic to the field $\mathbb{Z}_2(\omega)[x]/\langle x^2 + x + \omega\rangle$, so that $\alpha^2 + \alpha + \omega = 0$. Show that $1 + \alpha$ is a primitive element of $\mathbb{Z}_2(\omega, \alpha)$.

(c) Use $1 + \alpha$ to find an irreducible polynomial of degree 4 over $\mathbb{Z}_2$.

Solution

(a) We have $f(0) = \omega$, $f(1) = \omega$, $f(\omega) = 1 + \omega$ and $f(1 + \omega) = 1 + \omega$. It follows that $f(x)$ has no linear factors and, since it is a quadratic polynomial, it is irreducible.

(b) The multiplicative group of $\mathbb{Z}_2(\omega, \alpha)$ has order $2^4 - 1$, that is, 15. Hence we need to show that $1 + \alpha$ has order 15. If it does not have order 15 it will have order 3 or 5, so we only need to check these powers of $1 + \alpha$. We will, however, calculate all the powers up to 5, as they will be needed in the final part of the solution. Since we are working modulo 2 and since $\omega^2 = \omega + 1$ and $\alpha^2 = \alpha + \omega$, we have

$$(1 + \alpha)^2 = 1 + \omega + \alpha$$
$$(1 + \alpha)^3 = 1 + \alpha + \omega\alpha$$
$$(1 + \alpha)^4 = \alpha$$
$$(1 + \alpha)^5 = \omega.$$

Since $1+\alpha$ does not have order 1, 3 or 5, it must have order 15 and it is, therefore, primitive.

(c) We wish to find $a, b, c, d, e \in \mathbb{Z}_2$, not all zero, such that

$$a + b(1+\alpha) + c(1+\alpha)^2 + d(1+\alpha)^3 + e(1+\alpha)^4 = 0.$$

Using the calculations in part (b) reduce this equation to

$$(a+b+c+d) + c\omega + (b+c+d+e)\alpha + d\omega\alpha = 0.$$

We know from the proof of Theorem 2.29 that the set $\{1, \omega, \alpha, \omega\alpha\}$ is linearly independent. Hence we deduce that $c = d = 0$ and so $a + b = 0$ and $b + e = 0$. There is just one non-zero solution, namely $a = b = e = 1$.

Thus, an irreducible polynomial of degree 4 over $\mathbb{Z}_2$ is $x^4 + x + 1$.

Learning outcomes

We list those topics on which we may set assessment questions to test your understanding of the chapter.

After working through this chapter you should be able to:

(a) Carry out calculations in various fields, including finite fields.

(b) Show given field extensions are isomorphic and show given field extensions are not isomorphic.

(c) Write down the basis for E as a field extension of a field F in simple cases.

(d) Find the minimal polynomial for an algebraic element over a field in simple cases.

(e) Find the inverse of elements in a given field extension.

(f) Determine whether a polynomial is irreducible over a given field in simple cases.

(g) Determine the splitting field of a polynomial over a field in simple cases.

(h) Determine whether a given element of $\mathbb{Z}_n$ and simple extensions is a primitive element.

Solutions to exercises

Solution to Exercise 1.1

We know from Proposition 4.14 of Chapter 17 that $\mathrm{Im}(f)$ is a ring. Since $\mathrm{Im}(f) \neq \{0\}$, by the solution to Exercise 1.4 of Book C, Chapter 11, the additive and multiplicative identities are distinct. To show that $\mathrm{Im}(f)$ is a field we must check that non-zero elements have multiplicative inverses in $\mathrm{Im}(f)$.

Let $r \in \mathrm{Im}(f)$ be such that $r \neq 0$. Then $r = f(s)$ for some $s \in F$, $s \neq 0$. Since F is a field, s has an inverse $s^{-1} \in F$. By Proposition 1.1 we then have $f(s^{-1}) = f(s)^{-1} = r^{-1}$ and hence $\mathrm{Im}(f)$ is a field.

Now $\mathrm{Ker}(f)$ is an ideal in F, and we know from the solution to Exercise 2.5 in Chapter 17 that the only ideals in F are $\{0\}$ or F itself. As $f \neq 0$, $\mathrm{Ker}(f)$ cannot be the whole field, so $\mathrm{Ker}(f) = \{0\}$. The First Isomorphism Theorem (Chapter 17, Theorem 4.17) gives $F/\mathrm{Ker}(f) \cong \mathrm{Im}(f)$. But since $\mathrm{Ker}(f) = \{0\}$, this implies that $F \cong \mathrm{Im}(f)$, as required.

Solution to Exercise 1.2

(a) Since there is no $\beta \in \mathbb{Z}$ with $p(\beta) = 0$, $p(x)$ has no linear factors and so it is irreducible by Gauss's Lemma.

(b) Although we could divide the product of two linear polynomials by $p(x)$ and find the remainder, we can instead use the fact that $\alpha^2 = \alpha - 1 \pmod{p(\alpha)}$. This is because

$$\begin{aligned}\alpha^2 &= x^2 + \langle p(x)\rangle \\ &= x^2 - x + 1 - (-x+1) + \langle p(x)\rangle \\ &= x - 1 + \langle p(x)\rangle.\end{aligned}$$

We can then calculate the product directly:

$$\begin{aligned}(a+b\alpha)(c+d\alpha) &= ac + (ad+bc)\alpha + bd\alpha^2 \\ &= ac + (ad+bc)\alpha + bd(\alpha - 1) \pmod{p(\alpha)} \\ &= ac - bd + (ad+bc+bd)\alpha \pmod{p(\alpha)}.\end{aligned}$$

Thus the multiplication rule for elements of E in the required representation is given by

$$(a+b\alpha)(c+d\alpha) = ac - bd + (ad+bc+bd)\alpha.$$

Solution to Exercise 1.3

(a) Since 5 and 6 are quadratic non-residues of 7, x^2-5 and x^2-6 are irreducible polynomials in $\mathbb{Z}_7[x]$. Hence $\mathbb{Z}_7[x]/\langle x^2-5\rangle$ and $\mathbb{Z}_7[x]/\langle x^2-6\rangle$ are fields by Proposition 1.5.

(b) By Proposition 1.7, the elements of $\mathbb{Z}_7[x]/\langle x^2-5\rangle$ can be written as $a+b\sqrt{5}$ where $a,b\in\mathbb{Z}_7$ and those of $\mathbb{Z}_7[x]/\langle x^2-6\rangle$ can be written as $c+d\sqrt{6}$ where $c,d\in\mathbb{Z}_7$.

We wish to define $\psi(a+b\sqrt{5})$ so that $\psi:\mathbb{Z}_7[x]/\langle x^2-5\rangle\to\mathbb{Z}_7[x]/\langle x^2-6\rangle$ is an isomorphism. In other words, we need to define $\psi(\sqrt{5})=r+s\sqrt{6}$ where $(r+s\sqrt{6})^2\equiv 5\pmod 7$.

Thus we require r and s such that

$$(r+s\sqrt{6})^2=r^2+6s^2+2rs\sqrt{6}\equiv 5 \pmod 7.$$

This implies that either r or s is zero. Since we know that 5 is a quadratic non-residue of 7, we have $r=0$. Thus we require s with $6s^2\equiv 5\pmod 7$, that is, such that $s^2\equiv 2\pmod 7$. Now 2 is a quadratic residue of 7 with $3^2\equiv 2\pmod 7$, so we can choose $s=3$.

Let $\psi(a+b\sqrt{5})=a+3b\sqrt{6}$ so that $\psi^{-1}(c+d\sqrt{6})=c+5d\sqrt{5}$, as $3\times 5\equiv 1\pmod 7$. Hence ψ is a bijection, and since $\psi(1)=1$ we just need to show the isomorphism properties for addition and multiplication.

For addition we have

$$\begin{aligned}\psi(a+b\sqrt{5})+\psi(c+d\sqrt{5}) &= a+3b\sqrt{6}+c+3d\sqrt{6}\\ &= (a+c)+3(b+d)\sqrt{6}\\ &= \psi(a+c+(b+d)\sqrt{5})\\ &\equiv \psi((a+b\sqrt{5})+(c+d\sqrt{5})) \pmod 7.\end{aligned}$$

For multiplication we have

$$\begin{aligned}\psi(a+b\sqrt{5})\psi(c+d\sqrt{5}) &= (a+3b\sqrt{6})(c+3d\sqrt{6})\\ &\equiv ac+5bd+3(ad+bc)\sqrt{6} \pmod 7\end{aligned}$$

since $54\equiv 5\pmod 7$, and

$$\begin{aligned}\psi((a+b\sqrt{5})(c+d\sqrt{5})) &= \psi(ac+5bd+(ad+bc)\sqrt{5})\\ &\equiv ac+5bd+3(ad+bc)\sqrt{6} \pmod 7.\end{aligned}$$

Thus ψ is a field isomorphism.

Solution to Exercise 1.4

(a) The degree of $x-2$ is 1, so by Proposition 1.7 $\mathbb{Q}[x]/\langle x-2\rangle$ is a field whose elements can be written in the form a for $a\in\mathbb{Q}$. The result follows.

(b) By the Fundamental Theorem of Algebra, the only irreducible polynomials in $\mathbb{C}[x]$ are polynomials of the form $x-\alpha$ where $\alpha\in\mathbb{C}$. The result follows as in part (a).

Solution to Exercise 1.5

Let $f\colon \mathbb{Z}_p \to F$ be defined by

$$f(n) = \underbrace{1+1+\cdots+1}_{n \text{ terms}}.$$

By the properties of addition and multiplication in $\mathbb{Z}_p$ and in F, f is a homomorphism and $\mathrm{Im}(f) = K$. The required result follows since the image of a field is a field by Exercise 1.1.

Solution to Exercise 2.1

Since any $a + b\alpha \in E$ can be written as $a \cdot 1 + b \cdot \alpha$, $\{1, \alpha\}$ is a spanning set. Since the elements of E are uniquely expressed in the form $a + b\alpha$, where $a, b \in \mathbb{Q}$, $a + b\alpha = 0$ only when $a = b = 0$, and so the set $\{1, \alpha\}$ is linearly independent. Thus $\{1, \alpha\}$ is a basis for E as a vector space over F.

There are many other bases, but $\{1, \alpha\}$ is a rather natural one to consider.

Solution to Exercise 2.2

Let $m(x)$ be the minimal polynomial for α over F. Then $m(x)$ is a monic polynomial of lowest degree for which $m(\alpha) = 0$.

Therefore $\deg h(x) \geq \deg m(x)$, and so by the Division Algorithm for polynomials over a field we can write

$$h(x) = q(x)m(x) + r(x),$$

where $\deg r(x) < \deg m(x)$. Since $h(\alpha) = m(\alpha) = 0$ we have that $r(\alpha) = 0$. But as $m(x)$ is the smallest non-zero polynomial satisfying $m(\alpha) = 0$, we conclude that $r(x) = 0$ and so $h(x) = q(x)m(x)$. As $h(x)$ is monic and irreducible, this is only possible if $h(x) = m(x)$.

Solution to Exercise 2.3

(a) $x^2 + 1$

(b) (i) Since neither 2 nor 3 is a quadratic residue in $\mathbb{Z}_5$, the minimal polynomials are $x^2 - 2$ and $x^2 - 3$ respectively.

(ii) In $\mathbb{Z}_5(\beta)$ we have that $(2\beta)^2 = 4\beta^2 = 2 \pmod 5$ and $(3\beta)^2 = 9\beta^2 = 2 \pmod 5$, so $\alpha \in \mathbb{Z}_5(\beta)$ and $\mathbb{Z}_5(\alpha) \subseteq \mathbb{Z}_5(\beta)$. Since both extensions have degree 2 over $\mathbb{Z}_5$ by Theorem 2.21(c), a basis for $\mathbb{Z}_5(\alpha)$ is also a basis for $\mathbb{Z}_5(\beta)$, and so the two extensions must in fact be equal.

Solution to Exercise 2.4

As neither 1 nor -1 are roots of the equation $x^3 - 3x - 1 = 0$, by the Rational Root Test (Book C, Chapter 11, Theorem 4.7), the polynomial has no linear factors and so it is irreducible over $\mathbb{Q}$. As it is monic, it is the minimal polynomial for α. Since it has degree 3, the degree of the extension $\mathbb{Q}(\alpha)$ over $\mathbb{Q}$ is 3 by Theorem 2.21(c).

Solution to Exercise 2.5

Let $m(x)$ be the polynomial obtained by dividing $h(x)$ through by the leading coefficient. Then $m(x)$ is a monic and irreducible polynomial with $m(\alpha) = m(\beta) = 0$. Thus $m(x)$ is the minimal polynomial for both α and β by the solution to Exercise 2.2. The required result follows by Theorem 2.21.

Alternatively, the result follows from a direct allocation of Corollary 2.23.

Solution to Exercise 2.6

The solution to Worked Exercise 1.8 showed that $\mathbb{Z}_{13}(\sqrt{2}) \cong \mathbb{Z}_{13}(\sqrt{5})$. It is not difficult to see that the map from $\mathbb{Z}_{13}(\sqrt{t})$ to $\mathbb{Z}_{13}(\sqrt{-t})$ defined by $a + b\sqrt{t} \mapsto a + b\sqrt{-t}$ is an isomorphism, so we only need to show that $\mathbb{Z}_{13}(\sqrt{2}) \cong \mathbb{Z}_{13}(\sqrt{6})$. We use the same approach as in Worked Exercise 1.8 to work out the image of $\sqrt{2}$ under an isomorphism $\phi : \mathbb{Z}_{13}(\sqrt{2}) \mapsto \mathbb{Z}_{13}(\sqrt{6})$.

Let $\phi(\sqrt{2}) = a + b\sqrt{6}$. Then $2 = (a + b\sqrt{6})^2 = a^2 + 6b^2 + 2ab\sqrt{6}$, so $a = 0$ or $b = 0$. If $a = 0, 6b^2 = 2$ and so $3b^2 = 1$ and so $b^2 = 9$ and $b = 3$ (or 10). Thus we let $\phi(\sqrt{2}) = 3\sqrt{6}$, and so $\phi(a + b\sqrt{2}) = a + 3b\sqrt{6}$. The morphism property for addition is clear. We just need to check the property for multiplication:

$$\begin{aligned}\phi(a + b\sqrt{2})\phi(c + d\sqrt{2}) &= (a + 3b\sqrt{6})(c + 3d\sqrt{6}) \\ &= (ac + 2bd) + (3(bc + ad)\sqrt{6}) \\ &= \phi(ac + 2bd + (bc + ad)\sqrt{2}) \\ &= \phi[(a + b\sqrt{2})(c + d\sqrt{2})].\end{aligned}$$

Since the homomorphism property holds for both addition and multiplication, ϕ is an isomorphism, as required.

Solution to Exercise 2.7

The quadratic formula shows that $j = \dfrac{2 \pm \sqrt{-4}}{2} = 1 \pm i$ and so $j \in \mathbb{Q}(i)$. Thus $\mathbb{Q}(j) \subseteq \mathbb{Q}(i)$. Since $[\mathbb{Q}(i) : \mathbb{Q}] = [\mathbb{Q}(j) : \mathbb{Q}] = 2$, this is only possible if $\mathbb{Q}(j) = \mathbb{Q}(i)$.

Solution to Exercise 2.8

Suppose, by way of contradiction, that $\phi : \mathbb{Q}(\xi) \mapsto \mathbb{Q}(\eta)$ is an isomorphism sending ξ to $a + b\eta$ for some $a, b \in \mathbb{Q}$. Since both fields are subfields of $\mathbb{C}$, we know from Theorem 1.14 that $\phi(x) = x$ for all $x \in \mathbb{Q}$. In particular $\phi(-2) = -2$ so that

$$-2 = \phi(\xi^2) = (\phi(\xi))^2 = a^2 + 2ab\eta + b^2\eta^2 = a^2 + 2b^2 + 2b(a + b)\eta,$$

since $\eta^2 = 2\eta + 2$.

Since $\{1, \eta\}$ is a basis for $\mathbb{Q}(\eta)$, we can compare coefficients and deduce that $a^2 + 2b^2 = -2$, which is impossible for $a, b \in \mathbb{Q}$. So the fields $\mathbb{Q}(\xi)$ and $\mathbb{Q}(\eta)$ are not isomorphic.

Solution to Exercise 2.9

(a) We have $\mathbb{Q}(\sqrt{2}) = \mathbb{Q}(-\sqrt{2})$, since $-\sqrt{2} = (-1) \times \sqrt{2} \in \mathbb{Q}(\sqrt{2})$ and $\sqrt{2} = (-1) \times (-\sqrt{2}) \in \mathbb{Q}(-\sqrt{2})$.

(b) Elements of $\mathbb{Q}(\sqrt{-2})$ have the form $a + bj$ where $j^2 = -2$. Suppose that there is an isomorphism $\phi\colon \mathbb{Q}(\sqrt{2}) \to \mathbb{Q}(\sqrt{-2})$. Then $\phi(\sqrt{2}) = a + bj$ for some $a, b \in \mathbb{Q}$. Since $\phi(2) = 2$ we have

$$2 = \phi(2) = \phi(\sqrt{2})\phi(\sqrt{2}) = (a + bj)^2 = a^2 - 2b^2 + 2abj.$$

From this we can see that $a = 0$ or $b = 0$. If $b = 0$ then $a^2 = 2$, which is not possible for $a \in \mathbb{Q}$. If $a = 0$ then $-2b^2 = 2$, which is not possible, either, for $b \in \mathbb{Q}$. Hence there can be no isomorphism ϕ and $\mathbb{Q}(\sqrt{2}) \ncong \mathbb{Q}(\sqrt{-2})$.

Solution to Exercise 2.10

Since $(a + b\sqrt{2})^2 = a^2 + 2b^2 + 2ab\sqrt{2}$, if $(a + b\sqrt{2})^2 = 3$ then either $a = 0$ or $b = 0$. If $a^2 = 0$ then $b^2 = \frac{3}{2}$ and so $(2b)^2 = 6$, which is not possible for $b \in \mathbb{Q}$. If $b^2 = 0$ then $a^2 = 3$, which is not possible, either, for $a \in \mathbb{Q}$.

Thus, there are no $a, b \in \mathbb{Q}$ such that $(a + b\sqrt{2})^2 = 3$. Hence $x^2 - 3$ is irreducible over L. This shows that $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2})] = 2$. Since $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$, Theorem 2.29 implies that $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = 4$.

Solution to Exercise 3.1

(a) For any $u^j \in U$ we have $(u^j)^d = (u^d)^j = 1$, and so u^j is a root of $x^d - 1$.

(b) If $u^i = u^j$, then $u^{j-i} = 1$, which is impossible since $0 < j - i < d$ and u has order d.

Solution to Exercise 3.2

Let $\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$ and suppose that $n = rd$. Then r has order d and $\{r, 2r, \ldots, (d-1)r\}$ are the only elements whose order divides d. If s and d have a common factor t $(\neq 1)$, say, then the order of sr divides $\frac{d}{t}$, since $\frac{sd}{t}$ is a multiple of d. Otherwise sr has order d. Thus, all elements of order exactly d in the additive group $\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$ have the form sr, where $n = rd$, $1 \leq s \leq d$ and s and d are relatively prime. Hence the number of elements of order d in $(\mathbb{Z}_n, +)$ is equal to $\phi(d)$.

Solution to Exercise 3.3

(a) $(1 + i)$, $(1 + i)^2 = 2i$, $(1 + i)^3 = 1 + 2i$, $(1 + i)^4 = 2$, $(1 + i)^5 = 2 + 2i$, $(1 + i)^6 = i$, $(1 + i)^7 = 2 + i$, $(1 + i)^8 = 1$. (Remember that here arithmetic is modulo 3.)

(b) By part (a), $1 + i$ is a primitive element. Moreover, so are $(1 + i)^3 = 1 - i = 1 + 2i$, $(1 + i)^5 = 2 + 2i$ and $(1 + i)^7 = 2 + i$, as $3, 5$ and 7 are all coprime to 8.

Solution to Exercise 3.4

The possible orders of an element of $\mathbb{Z}_5^*$ are 1, 2 and 4, so it is enough to check that $2^2 \not\equiv 1 \pmod 5$. In fact $2^2 \equiv 4 \pmod 5$, so 2 is a primitive element modulo 5.

The possible orders of an element of $\mathbb{Z}_{11}^*$ are 1, 2, 5 and 10, so it is enough to check that $2^2 \not\equiv 1 \pmod{11}$ and $2^5 \not\equiv 1 \pmod{11}$. In fact $2^2 \equiv 4 \pmod{11}$ and $2^5 \equiv 10 \pmod{11}$, so 2 is a primitive element modulo 11.

The possible orders of an element of $\mathbb{Z}_{13}^*$ are 1, 2, 3, 4, 6 and 12, so it is enough to check that $2^2, 2^3, 2^4, 2^6 \not\equiv 1 \pmod{13}$. Modulo 13 we have

$$2^2 \equiv 4,\ 2^3 \equiv 8,\ 2^4 \equiv 3,\ 2^6 \equiv 2^2 \cdot 2^4 \equiv 12,$$

so 2 is a primitive element modulo 13.

The possible orders of an element of $\mathbb{Z}_{19}^*$ are 1, 2, 3, 6, 9 and 18, so it is enough to check that $2^2, 2^3, 2^6, 2^9 \not\equiv 1 \pmod{19}$. Modulo 19 we have

$$2^2 \equiv 4,\ 2^3 \equiv 8,\ 2^6 \equiv 8^2 \equiv 7,\ 2^9 \equiv 2^3 \cdot 2^6 \equiv 8 \cdot 7 \equiv 18$$

so 2 is a primitive element modulo 19.

Solution to Exercise 3.5

The possible orders of an element of $\mathbb{Z}_7^*$ are 1, 2, 3 and 6, so it is enough to check that $3^2 \not\equiv 1 \pmod 7$ and $3^3 \not\equiv 1 \pmod 7$. In fact $3^2 \equiv 2 \pmod 7$ and $3^3 \equiv 6 \pmod 7$, so 3 is a primitive element modulo 7.

The possible orders of an element of $\mathbb{Z}_{17}^*$ are 1, 2, 4, 8 and 16, so it is enough to check that $3^8 \not\equiv 1 \pmod{17}$ (as this also covers the powers 2 and 4). In fact, $3^8 \equiv 16 \pmod{17}$, so 3 is a primitive element modulo 17.

The possible orders of an element of $\mathbb{Z}_{19}^*$ are 1, 2, 3, 6, 9 and 18, so it is enough to check that $3^6 \not\equiv 1 \pmod{19}$ and $3^9 \not\equiv 1 \pmod{19}$ (as these also cover the powers 2, 3 and 6). In fact $3^6 \equiv 7 \pmod{19}$ and $3^9 \equiv 18 \pmod{19}$, so 3 is a primitive element modulo 19.

Solution to Exercise 3.6

$2^n \pmod{11}$	1	2	3	4	5	6	7	8	9	10
n	10	1	8	2	4	9	7	3	6	5

(a) The non-zero elements of $\mathbb{Z}_{11}$ that are squares are $1, 3, 4, 5, 9$, and so the values of a for which $t^2 - a$ is irreducible will be $2, 6, 7, 8, 10$.

(b) All elements of $\mathbb{Z}_{11}$ are cubes, and so all polynomials $t^3 - a$ are reducible over $\mathbb{Z}_{11}$.

(c) The primitive elements are $2 = 2^1$, $6 = 2^9$, $7 = 2^7$, $8 = 2^3$. (These are the elements whose exponent as a power of 2 is coprime to 10.)

Solution to Exercise 3.7

$3^n \pmod{17}$	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
n	16	14	1	12	5	15	11	10	2	3	7	13	4	9	6	8

(a) The non-zero elements of $\mathbb{Z}_{17}$ that are squares are $1, 2, 4, 8, 9, 13, 15, 16$, and so the values of a for which $t^2 - a$ is irreducible are $3, 5, 6, 7, 10, 11, 12,$ 14.

(b) All elements of $\mathbb{Z}_{17}$ are cubes, and so all polynomials $t^3 - a$ (for $a \in \mathbb{Z}_{17}^*$) are reducible over $\mathbb{Z}_{17}$.

(c) The primitive elements are $3 = 3^1$, $5 = 3^5$, $6 = 3^{15}$, $7 = 3^{11}$, $10 = 3^3$, $11 = 3^7$, $12 = 3^{13}$, $14 = 3^9$. (These are the elements whose exponent as a power of 3 is coprime to 16.)

Solution to Exercise 3.8

By Proposition 3.9, $x^2 + 1$ is irreducible in $\mathbb{Z}_p[x]$. Thus by Theorem 2.19, the field $\mathbb{Z}_p[x]/\langle x^2 + 1\rangle$ can be regarded as an extension of $\mathbb{Z}_p$ containing p^2 elements that have the form $a + b\alpha$ where $a, b \in \mathbb{Z}_p$ and $\alpha^2 + 1 = 0$.

Solution to Exercise 4.1

(a) In $\mathbb{Z}_3$, $x^3 - 2 = (x - 2)^3$ (by Theorem 1.12), and so all the roots of $x^3 - 2$ are in $\mathbb{Z}_3$ and the splitting field is $\mathbb{Z}_3$ itself.

(b) In $\mathbb{Z}_5$, $x^3 - 2 = (x - 3)(x^2 + 3x + 4)$. Now $x^2 + 3x + 4$ has no roots in $\mathbb{Z}_5$, and so it is irreducible in $\mathbb{Z}_5[x]$. Thus, a splitting field is $\mathbb{Z}_5[x]/\langle x^2 + 3x + 4\rangle$.

Chapter 19

Fields and geometry

Introduction

There is a story mathematicians often tell about the construction of new numbers from old which goes like this. To construct the negative integers from the positive integers, we solve equations like $x + 1 = 0$; to construct the rational numbers from the integers we solve equations like $mx = n$, where m and n are integers; and to construct the complex numbers from the real numbers we solve equations like $x^2 = -1$. (The real numbers do not fit into this story.) This is not an accurate account of how these types of numbers were discovered, but it makes a substantial mathematical point: faced with a problem you have to solve, it can be useful to create objects that count as the answers. In all of these cases the 'new' numbers can be handled by analogy with the old ones.

In this chapter, we look at two aspects of this process. Firstly, we consider the numbers that arise as the roots of polynomial equations of any degree and with rational coefficients, that is, equations of the form

$$a_0x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n = 0,$$

where $a_i \in \mathbb{Q}$ for $i = 0, \ldots, n$. These numbers are called *algebraic numbers*, and we show that they form a field. Moreover, we give a standard technique for finding a polynomial equation satisfied by an algebraic number. The basic building blocks of the corresponding theory will be developed in the first half of this chapter.

Secondly, we turn to the algebraic version of a story that has its roots in the classical geometry of ancient Greece. Around the time of Euclid (the second and third century BC), geometric problems often involved constructions. A famous one asked for the construction of a square twice the area of a given square, and another asked for a method to divide a given line segment into a given number of equal subsegments.

Both these problems can be solved by the use of a straightedge (an unmarked ruler) and a compasses (for drawing circles). Difficulties, however, arose with analogous problems, such as the construction of a cube twice the volume of a given cube, and the problem of dividing a given circular arc (or, equivalently, a given angle) into three equal parts. Although the Greeks solved these problems geometrically, their solutions involved elaborate methods such as the use of conic sections, and no solutions were found using straightedge and compasses alone. When these two problems were revived in the modern West around the time of Descartes in the seventeenth century, it came to be believed that no solutions could be found by straightedge and compasses alone, and this was eventually shown to be the case by an otherwise little-known French mathematician, Pierre Wantzel, in 1837.

Alone in human investigation, mathematics offers the chance to prove that something is impossible; the other sciences can merely establish that something is very unlikely. But what allows mathematicians to prove that the cube cannot be doubled and the angle cannot be trisected by the required methods?

One clue comes from expressing geometric problems in algebraic terms. To find the side of cube that is double the volume of another (say, a cube of unit volume) is to find an x such that $x^3 = 2$. To express the problem of trisecting an angle of φ in algebraic terms we first recall the trigonometrical formula

$$\cos 3\theta = 4\cos^3\theta - 3\cos\theta.$$

If we set $3\theta = \varphi$ this equation becomes

$$\cos\varphi = 4\cos^3\left(\frac{\varphi}{3}\right) - 3\cos\left(\frac{\varphi}{3}\right),$$

which we regard as a cubic equation for $x = \cos(\frac{\varphi}{3})$ given the value, a say, of $\cos\varphi$:

$$4x^3 - 3x - a = 0.$$

On the other hand, when we make a geometric construction in the plane we know a line segment if, and only if, we know the coordinates of its endpoints. This means that we know all the line segments whose endpoints have rational coordinates: start from the segment that goes from the origin to the point $(1, 0)$ and copy it (by shifting and rotating) and divide it (using similar triangles) as necessary.

Thus, we can draw lines with rational slopes that pass through a point with rational coordinates by joining pairs of known points. Likewise, we can draw circles with their centres at points with rational coordinates and that have radii whose squares are rational, by taking one such point as the centre and the radius as a line segment from the first point to some other known point.

When one of these circles meets one of these lines we can get new points, whose coordinates simultaneously satisfy the equation of the line and the equation of the circle. As you might expect, the coordinates of these points generally involve square roots, because the equation of the circle contains squared terms and so the equations to be solved may well be quadratic equations. A similar result occurs when one of these circles meets another of these circles.

Now, a geometric construction involves a sequence of operations each of which involves drawing either a circle or a line, and at each stage the only points available are the ones already constructed. So at each stage we construct points whose coordinates are either rational numbers, or square roots of rational numbers, or square roots of numbers that involve square roots of rational numbers, and so on. At each stage the new coordinates are obtained by solving a family of linear and quadratic equations, and the roots might be rational, or roots of an equation of degree 2, or roots of an equation of degree 4, and so on.

But a cubic equation is surely unlikely to arise in this way, and if we can show that no (irreducible) cubic equation arises, then we have indeed proved that the cube cannot be doubled in volume, nor the angle trisected, by straightedge and compasses alone, all because 3 is not a power of 2.

The second half of this chapter is given over to establishing how such proofs can be achieved.

Chapter guide

The first section of this chapter revises and develops the material of Chapter 18. It will require reasonable fluency at working with polynomials. You will also need to be able to carry out Gaussian elimination to find the determinant of a matrix. There is a worked exercise that should help you with this.

The second section is about ruler and compasses constructions and involves elementary geometry. You may find it helpful to actually do the constructions using paper and pencil. The text states key results from geometry as they are needed.

1 Field extensions revisited

The field extensions introduced and discussed in Chapter 18 were obtained by adjoining a finite number of elements to the base field – usually, just a single element. The solution to the first exercise of this chapter will enable us to generalise this construction to extensions by arbitrary sets of elements.

Exercise 1.1

Let F be a subfield of a field E and let S be a subset of elements of E. Let L be the intersection $\bigcap M_i$ of all the subfields M_i of E that contain both S and F. Show that

(a) L is a subfield of E

(b) if K is a subfield of E with $F \subseteq K$ and $S \subseteq K$ then L is a subfield of K.

Note that the index i in M_i is for notational convenience. You should not assume that it is an integer as there could be an uncountably infinite number of such fields.

Exercise 1.1 allows us to define the subfield generated by a set.

Definition 1.1 *Subfield generated by a set*

Let F be a subfield of a field E and let S be a subset of elements of E. We define $F(S)$ to be the smallest subfield of E containing F and all the elements of S. If no field F is specified, then the smallest subfield of E that contains S is called the subfield of E **generated** by S.

Exercise 1.1 tells us that $F(S) = \bigcap M_i$, where the M_i range over all the subfields of E that contain both S and F.

In order to match the notation introduced in Chapter 18, when $S = \{s_1, \ldots, s_k\}$ is a finite set, we write $F(S) = F(s_1, \ldots, s_k)$ instead of $F(\{s_1, \ldots, s_k\})$.

Our aim is to show that finite-dimensional extensions are necessarily algebraic. We start by proving a simple necessary and sufficient condition for an element to be algebraic.

Theorem 1.2

Let E be an extension of a field F. An element α of E is algebraic over F if, and only if, the degree $[F(\alpha) : F]$ is finite.

Proof Let the degree $[F(\alpha) : F]$ be finite. This implies that the vector space $F(\alpha)$ has a finite dimension n, say, over F. Consequently, any set of $n + 1$ elements of K must be linearly dependent over F. Consider a particular set of consecutive powers of α for such a set, namely, $\{1, \alpha, \alpha^2, \ldots, \alpha^n\}$. Since this set of $n + 1$ elements is linearly dependent, there exist coefficients $c_0, c_1, c_2, \ldots, c_n \in F$, at least one of which is non-zero, such that

$$c_0 + c_1\alpha + c_2\alpha^2 + \cdots + c_n\alpha^n = 0.$$

Since at least one coefficient c_j is non-zero, the above equation shows that α is a root of a non-zero polynomial over F.

Conversely, let $\alpha \in E$ be a root of a polynomial over F. Then, by Theorem 2.21(c) of Chapter 18, α is a root of an irreducible polynomial over F and the degree $[F(\alpha) : F]$ is finite (and equal to the degree of the irreducible polynomial that has α as a root). ■

Exercise 1.2

Show that if F is a subfield of E and $\alpha \in E$ is algebraic over F and if K is any field such that $F \subset K \subset E$, then α is also algebraic over K.

We are now ready to prove a main result that characterises field extensions of finite degree.

Theorem 1.3 *Field extensions of finite degree*

Let $F \subset E$ be fields. Then the degree $[E : F]$ is finite if, and only if, E is an algebraic extension of F and there exists a finite subset S of E such that $E = F(S)$.

Proof Suppose that $[E : F]$ is finite, say equal to n. This implies that E, regarded as a vector space over the field F, has a basis $S = \{\beta_1, \beta_2, \ldots, \beta_n\}$ consisting of elements of E. Now $F \subseteq E$ and $S \subseteq E$ and so $F(S) \subseteq E$. Since every element of E can be expressed in the form $c_1\beta_1 + c_2\beta_2 + \cdots + c_n\beta_n$ for some $c_1, c_2, \ldots, c_n \in F$, it is also the case that $E \subseteq F(S)$ because $F(S)$ is a field and so closed under addition. Hence $E = F(S)$.

Suppose that α is an arbitrary element of E. Then $F(\alpha) \subset E$ and so, by Theorem 2.29 of Chapter 18, $[F(\alpha) : F] \leq [E : F] = n$. This implies that the degree $[F(\alpha) : F]$ is finite and so α is algebraic over F by Theorem 1.2.

Conversely, suppose that E is an algebraic extension of F and that there is $S = \{s_1, s_2, \ldots, s_k\}$ with $E = F(S)$. Since E is an algebraic extension, all the elements in S are algebraic over F and hence, by the solution to Exercise 1.2, they are algebraic over any field L such that $F \subset L \subset E$.

From Theorem 1.2 we know that the degrees $[L(s_j) : L]$ are finite for any j such that $1 \leq j \leq k$, and for any field L such that $F \subset L \subset E$. It follows that if $L_j = F(s_1, \ldots, s_{j-1})$ for $1 \leq j \leq k$, then the degrees $[L_j(s_j) : L_j]$ are all finite.

We now apply Theorem 2.29 of Chapter 18 to the chain of fields

$$F \subseteq F(s_1) \subseteq F(s_1, s_2) \subseteq \cdots \subseteq F(S) = E$$

to obtain

$$[E : F] = [F(s_1) : F][F(s_1, s_2) : F(s_1)] \cdots [F(S) : F(s_1, s_2, \ldots, s_{k-1})] .$$

Since all the factors on the right-hand side are finite, we conclude that $[E : F]$ is finite. ■

1.1 Algebraic extensions revisited

The next two subsections develop some techniques for doing calculations in algebraic extensions. This subsection starts with an exercise that extends the idea of 'rationalisation' to help find inverses of elements in $\mathbb{Q}(\sqrt{2}, \sqrt{3})$. Consider an element $a + b\sqrt{3} \in \mathbb{Q}(\sqrt{2}, \sqrt{3})$ with $a, b \in \mathbb{Q}(\sqrt{2})$. We can write

$$\frac{1}{a + b\sqrt{3}} = \frac{a - b\sqrt{3}}{a^2 - 3b^2}$$

by multiplying both the numerator and the denominator of the fraction on the left-hand side by $a - b\sqrt{3}$. The important observation is that the denominator of the fraction on the right-hand side now only involves elements of $\mathbb{Q}[\sqrt{2}]$. We can repeat the process by multiplying top and bottom by appropriate expressions so that the denominator eventually becomes an element of $\mathbb{Q}$.

Exercise 1.3

Let $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$.

(a) By writing $1 + \sqrt{2} + 2\sqrt{3} + \sqrt{6}$ as $1 + \sqrt{2} + (2 + \sqrt{2})\sqrt{3}$, show that

$$\frac{1}{1 + \sqrt{2} + 2\sqrt{3} + \sqrt{6}} = \frac{1 + \sqrt{2} - 2\sqrt{3} - \sqrt{6}}{-15 - 10\sqrt{2}}.$$

(b) Find the inverse of $1 + \sqrt{2} + 2\sqrt{3} + \sqrt{6}$ in the form $a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}$ where $a, b, c, d \in \mathbb{Q}$.

The next worked exercise and the following exercise explore the field $\mathbb{Q}(\sqrt{2}, \sqrt{3})$.

Worked Exercise 1.4 *A polynomial over $\mathbb{Q}$ with root $\sqrt{2} + \sqrt{3}$*

Consider the field $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. In the solution to Exercise 2.10 of Chapter 18 we saw that $[K : \mathbb{Q}] = 4$. By Theorem 1.3 every element of K is algebraic over $\mathbb{Q}$. This implies that the element $\sqrt{2} + \sqrt{3}$ is itself algebraic over $\mathbb{Q}$. Since the degree $[K : \mathbb{Q}]$ is 4, the number $\sqrt{2} + \sqrt{3}$ is a root of some polynomial of degree at most 4 over $\mathbb{Q}$. Find such a polynomial.

Solution

We first note that $(\sqrt{2} + \sqrt{3})^2 = 5 + 2\sqrt{6}$ and that $(5 + 2\sqrt{6})(5 - 2\sqrt{6}) = 1 \in \mathbb{Q}$. The latter observation gives

$$(y - (5 + 2\sqrt{6}))(y - (5 - 2\sqrt{6})) = y^2 - 10y + 1.$$

Thus a suitable polynomial is $x^4 - 10x^2 + 1$.

Since a factorisation in $\mathbb{R}$ is $(x^2 - (5 + 2\sqrt{6}))(x^2 - (5 - 2\sqrt{6}))$ and the factors are not in $\mathbb{Q}[x]$, this polynomial is irreducible over $\mathbb{Q}$. Since it is monic, by Exercise 2.2 in Chapter 18, this is the minimal polynomial for $\sqrt{2} + \sqrt{3}$ over $\mathbb{Q}$.

In Worked Exercise 1.4 we found a polynomial equation over the field $\mathbb{Q}$ for $\sqrt{2} + \sqrt{3}$ by using specific algebraic properties of this element. In the next subsection we will develop a reasonably fast method for determining a polynomial over a given field with a root outside the field that does not depend on such algebraic properties.

Exercise 1.4

(a) Determine all the roots of the polynomial $x^4 - 10x^2 + 1$.

(b) Show that $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$.

(c) Show that this field is the splitting field of the irreducible polynomial $x^4 - 10x^2 + 1$.

1.2 The field of algebraic numbers

Suppose that a field E is an extension of a field F. Our next aim is to study the collection of all elements of E that are algebraic over F. We start by proving that this set is closed under addition and multiplication.

Theorem 1.5

Let $F \subset E$ be fields and let $\alpha, \beta \in E$ be algebraic over F. Then both $\alpha + \beta$ and $\alpha\beta$ are elements of E that are algebraic over F.

Proof If α and β are algebraic over F, then β is also algebraic over $F(\alpha)$ by Exercise 1.2. Applying Theorem 2.29 of Chapter 18 to the chain of fields

$$F \subset F(\alpha) \subset F(\alpha, \beta)$$

gives

$$[F(\alpha, \beta) : F] = [F(\alpha, \beta) : F(\alpha)][F(\alpha) : F].$$

Since both factors on the right-hand side are finite, the degree $[F(\alpha, \beta) : F]$ is finite. By Theorem 1.3, every element in $F(\alpha, \beta)$ must be algebraic over F. But $\alpha + \beta$ and $\alpha\beta$ both belong to $F(\alpha, \beta)$, and hence they are algebraic. ■

One consequence of Theorem 1.5 is that whenever α and β are roots of a polynomial over a field F, the elements $\alpha + \beta$ and $\alpha\beta$ are also roots of some polynomial over F. In Example 1.4 you saw a way of finding such a polynomial where $F = \mathbb{Q}, \alpha = \sqrt{2}$ and $\beta = \sqrt{3}$. We now address the question of doing this in full generality.

The idea is as follows. Let $F \subseteq E$ with $[E : F] = n$ and let $\alpha \in E \backslash F$. Then the $n + 1$ elements $1, \alpha, \alpha^2, \ldots, \alpha^n$ are linearly dependent in the n-dimensional vector space E over the field F. The linear dependence means that there are $n + 1$ elements $c_0, c_1, c_2, \ldots, c_n \in F$, not all zero, such that

$$c_0 1 + c_1\alpha + c_2\alpha^2 + \cdots + c_n\alpha^n = 0,$$

from which a polynomial equation for α can be extracted.

However, it may not be obvious to you at this moment how this idea works in practice for more complicated algebraic elements, such as, for instance, $\alpha = \sqrt{2} + \sqrt[3]{2}$. The next worked example illustrates this approach for this particular element. The method avoids direct calculations of high powers of α and, at the same time, it provides an interesting application of certain elementary facts from linear algebra regarding linear dependence, homogeneous linear systems and determinants (known to you from earlier modules, albeit only over the field of real numbers).

Worked Exercise 1.6

Find a polynomial over $\mathbb{Q}$ with root $\sqrt{2} + \sqrt[3]{2}$.

Solution

By Theorem 1.5, the number $\alpha = \sqrt{2} + \sqrt[3]{2}$ is algebraic over $\mathbb{Q}$. Now $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$ and $\sqrt[3]{2}$ is a root of $x^3 - 2$. Since $x^3 - 2$ is monic and irreducible, it is the minimal polynomial for $\sqrt[3]{2}$ over $\mathbb{Q}$, and so any finite field extension of $\mathbb{Q}$ containing this root must have degree a multiple of 3. Thus $[\mathbb{Q}(\sqrt{2}, \sqrt[3]{2}) : \mathbb{Q}(\sqrt{2})] = 3$ and so by Theorem 2.29 from Chapter 18 (the KLM Theorem), we have $[\mathbb{Q}(\sqrt{2}, \sqrt[3]{2}) : \mathbb{Q}]$ is 6.

Hence, since $\alpha \in \mathbb{Q}(\sqrt{2}, \sqrt[3]{2})$, the element α is a root of a polynomial over $\mathbb{Q}$ of degree at most 6. As in the proof of the KLM Theorem, a basis for the vector space $\mathbb{Q}(\sqrt{2}, \sqrt[3]{2})$ over the field $\mathbb{Q}$ is $B = \{u_1, u_2, \ldots, u_6\}$, where

$$u_1 = 1,\ u_2 = \sqrt[3]{2},\ u_3 = \sqrt[3]{4},\ u_4 = \sqrt{2},\ u_5 = \sqrt{2} \cdot \sqrt[3]{2},\ u_6 = \sqrt{2} \cdot \sqrt[3]{4}.$$

Now, every element of E can be expressed as a linear combination of elements of B with coefficients in F in a unique way. In particular, this applies to the six elements $u_1\alpha, u_2\alpha, \ldots, u_6\alpha$. Our first step is to find these linear combinations, which we do by direct calculation.

$$\begin{aligned}
u_1\alpha &= \sqrt{2} + \sqrt[3]{2} \\
u_2\alpha &= \sqrt{2}\sqrt[3]{2} + \sqrt[3]{4} \\
u_3\alpha &= \sqrt{2}\sqrt[3]{4} + 2 \\
u_4\alpha &= 2 + \sqrt{2}\sqrt[3]{2} \\
u_5\alpha &= 2\sqrt[3]{2} + \sqrt{2}\sqrt[3]{4} \\
u_6\alpha &= 2\sqrt[3]{4} + 2\sqrt{2}
\end{aligned}$$

Writing the right-hand sides of these equations in terms of $u_1, \ldots, u_6$ yields the following linear system.

$$\begin{aligned}
u_1\alpha &= 0 \cdot u_1 + 1 \cdot u_2 + 0 \cdot u_3 + 1 \cdot u_4 + 0 \cdot u_5 + 0 \cdot u_6 \\
u_2\alpha &= 0 \cdot u_1 + 0 \cdot u_2 + 1 \cdot u_3 + 0 \cdot u_4 + 1 \cdot u_5 + 0 \cdot u_6 \\
u_3\alpha &= 2 \cdot u_1 + 0 \cdot u_2 + 0 \cdot u_3 + 0 \cdot u_4 + 0 \cdot u_5 + 1 \cdot u_6 \\
u_4\alpha &= 2 \cdot u_1 + 0 \cdot u_2 + 0 \cdot u_3 + 0 \cdot u_4 + 1 \cdot u_5 + 0 \cdot u_6 \\
u_5\alpha &= 0 \cdot u_1 + 2 \cdot u_2 + 0 \cdot u_3 + 0 \cdot u_4 + 0 \cdot u_5 + 1 \cdot u_6 \\
u_6\alpha &= 0 \cdot u_1 + 0 \cdot u_2 + 2 \cdot u_3 + 2 \cdot u_4 + 0 \cdot u_5 + 0 \cdot u_6
\end{aligned}$$

Subtracting $u_i\alpha$ from both sides of each equation gives a homogeneous linear system of equations with the 6×6 coefficient matrix

$$\begin{pmatrix} -\alpha & 1 & 0 & 1 & 0 & 0 \\ 0 & -\alpha & 1 & 0 & 1 & 0 \\ 2 & 0 & -\alpha & 0 & 0 & 1 \\ 2 & 0 & 0 & -\alpha & 1 & 0 \\ 0 & 2 & 0 & 0 & -\alpha & 1 \\ 0 & 0 & 2 & 2 & 0 & -\alpha \end{pmatrix}.$$

Since we know that α is in the field and that α is not zero, we have a non-zero solution of this system, namely, the 6-tuple $u_1, \ldots, u_6$. This implies that the determinant of the matrix of this system must be equal to zero that is,

$$\begin{vmatrix} -\alpha & 1 & 0 & 1 & 0 & 0 \\ 0 & -\alpha & 1 & 0 & 1 & 0 \\ 2 & 0 & -\alpha & 0 & 0 & 1 \\ 2 & 0 & 0 & -\alpha & 1 & 0 \\ 0 & 2 & 0 & 0 & -\alpha & 1 \\ 0 & 0 & 2 & 2 & 0 & -\alpha \end{vmatrix} = 0.$$

Evaluating the determinant in terms of α gives a polynomial expression in terms of α, which in turn gives a polynomial equation satisfied by α.

We now perform elementary row and column operations to evaluate the determinant. Although some row operations do change the value of the determinant, by either changing the sign or multiplying by a constant, a zero determinant is not affected by any of these operations. We first observe that the top right-hand block of the determinant has the form of a 3×3 identity matrix. As a result, our first step swaps the three right-hand columns with the three left-hand ones. We then proceed with Gaussian elimination.

First we swap the first three columns:

$$\begin{vmatrix} 1 & 0 & 0 & -\alpha & 1 & 0 \\ 0 & 1 & 0 & 0 & -\alpha & 1 \\ 0 & 0 & 1 & 2 & 0 & -\alpha \\ -\alpha & 1 & 0 & 2 & 0 & 0 \\ 0 & -\alpha & 1 & 0 & 2 & 0 \\ 2 & 0 & -\alpha & 0 & 0 & 2 \end{vmatrix} = 0.$$

Next we clear the first column below the diagonal:

$$\begin{vmatrix} 1 & 0 & 0 & -\alpha & 1 & 0 \\ 0 & 1 & 0 & 0 & -\alpha & 1 \\ 0 & 0 & 1 & 2 & 0 & -\alpha \\ 0 & 1 & 0 & 2-\alpha^2 & \alpha & 0 \\ 0 & -\alpha & 1 & 0 & 2 & 0 \\ 0 & 0 & -\alpha & 2\alpha & -2 & 2 \end{vmatrix} \quad \begin{matrix} \\ \\ \\ r_4 = r_4 + \alpha r_1 \\ \\ r_6 = r_6 - 2r_1. \end{matrix}$$

Now we clear the second column below the diagonal:

$$\begin{vmatrix} 1 & 0 & 0 & -\alpha & 1 & 0 \\ 0 & 1 & 0 & 0 & -\alpha & 1 \\ 0 & 0 & 1 & 2 & 0 & -\alpha \\ 0 & 0 & 0 & 2-\alpha^2 & 2\alpha & -1 \\ 0 & 0 & 1 & 0 & 2-\alpha^2 & \alpha \\ 0 & 0 & -\alpha & 2\alpha & -2 & 2 \end{vmatrix} \quad \begin{matrix} \\ \\ \\ r_4 = r_4 - r_2 \\ r_5 = r_5 + \alpha r_2. \\ \end{matrix}$$

Clearing the third column below the diagonal gives

$$\begin{vmatrix} 1 & 0 & 0 & -\alpha & 1 & 0 \\ 0 & 1 & 0 & 0 & -\alpha & 1 \\ 0 & 0 & 1 & 2 & 0 & -\alpha \\ 0 & 0 & 0 & 2-\alpha^2 & 2\alpha & -1 \\ 0 & 0 & 0 & -2 & 2-\alpha^2 & 2\alpha \\ 0 & 0 & 0 & 4\alpha & -2 & 2-\alpha^2 \end{vmatrix} \quad \begin{matrix} \\ \\ \\ \\ r_5 = r_5 - r_3 \\ r_6 = r_6 + \alpha r_3. \end{matrix}$$

At this stage we stop as we can see that the equation we are seeking is equivalent to

$$\begin{vmatrix} 2-\alpha^2 & 2\alpha & -1 \\ -2 & 2-\alpha^2 & 2\alpha \\ 4\alpha & -2 & 2-\alpha^2 \end{vmatrix} = 0.$$

Evaluating this 3×3 determinant gives

$$(2-\alpha^2)[(2-\alpha^2)^2 + 4\alpha] - 2\alpha[-2(2-\alpha^2) - 8\alpha^2] \\ -[4 - 4\alpha(2-\alpha^2)] = 0,$$

which simplifies to

$$\alpha^6 - 6\alpha^4 - 4\alpha^3 + 12\alpha^2 - 24\alpha - 4 = 0.$$

It follows that $\alpha = \sqrt{2} + \sqrt[3]{2}$ is a root of the polynomial

$$x^6 - 6x^4 - 4x^3 + 12x^2 - 24x - 4.$$

We could have carried out further row operations to reduce our calculation to the evaluation of a 2×2 determinant, but it seemed easier to stop and evaluate the determinant directly.

The following strategy summarises the approach taken in Worked Exercise 1.6.

Strategy: to find a polynomial over F that has α as a root

Let E be an extension of a field F such that $[E:F] = n$ and let α be an element of E.

1. Write down a basis $B = \{u_1, \ldots, u_n\}$ for E as a vector space over F.
2. For $j = 1, \ldots, n$, express $u_j\alpha$ as a linear combination of elements of B, that is
$$u_j\alpha = c_{j,1}u_1 + \cdots + c_{j,j}u_j + \cdots + c_{j,n}u_n.$$
3. Rearrange the equations obtained in step 2 as
$$c_{j,1}u_1 + \cdots + (c_{j,j} - \alpha)u_j + \cdots + c_{j,n}u_n = 0.$$
4. Write down the coefficient matrix A of the resulting system of n homogeneous linear equations.
5. Since $u_1, u_2, \ldots, u_n$ is a non-zero solution for this system of equations, we know that $\det A = 0$.
6. The determinant $\det A$ will be a polynomial of degree at most n in α. This is the required polynomial.

Exercise 1.5

(a) Find a polynomial equation satisfied by $1 + \sqrt{2}$ in the field $\mathbb{Q}(\sqrt{2})$.

(b) Find a polynomial equation satisfied by $\sqrt{2} - \sqrt{3}$ in $\mathbb{Q}(\sqrt{2}, \sqrt{3})$.

Theorem 1.5 shows that the sum and the product of two algebraic elements over a field is again algebraic over the same field. In fact, the set of algebraic elements forms a subfield, as we will now prove.

Theorem 1.7

Let E and F be two fields such that $F \subset E$, and let A be the set of all the elements of E that are algebraic over F. Then A is a subfield of E.

Proof We will use the subfield criterion (Book C, Chapter 11, Lemma 1.21). By Theorem 1.5, for any $\alpha, \beta \in A$ we have $\alpha + \beta \in A$ and $\alpha\beta \in A$. In particular, from the latter we also see that $-\beta = (-1)\beta \in A$, and so $\alpha - \beta \in A$.

Let $\alpha \neq 0$ be a root of a polynomial $a_0 + a_1x + \cdots + a_{n-1}x^{n-1} + a_nx^n$ where $a_0, \ldots, a_n \in F$, so that

$$a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} + a_n\alpha^n = 0.$$

Then, since $\alpha^{-1} \in E$, taking out $\alpha^n \neq 0$ gives

$$\alpha^n(a_n + a_{n-1}\alpha^{-1} + \cdots + a_1(\alpha^{-1})^{n-1} + a_0(\alpha^{-1})^n) = 0\,.$$

Thus α^{-1} is a root of the polynomial $a_n + a_{n-1}x + \cdots + a_1x^{n-1} + a_0x^n$ and so $\alpha^{-1} \in A$.

Since the subset A of E is closed under the operations of addition and multiplication in E, contains 0 and 1, and is closed under taking additive and multiplicative inverses, the subfield criterion tells us that A is a subfield of the field E. ■

By the Fundamental Theorem of Algebra, any polynomial over $\mathbb{Q}$ has all its roots within $\mathbb{C}$, the field of complex numbers. Therefore, any algebraic number over $\mathbb{Q}$ is a complex number, but in fact we do not need to refer to $\mathbb{C}$ when we describe algebraic numbers over $\mathbb{Q}$; this observation and Theorem 1.7 enable us to make the following definition.

Definition 1.8 *Field of algebraic numbers*

Let E be an extension of a field F. The subfield of E that consists of all the elements of E that are algebraic over F is called the **field of algebraic numbers in E over F** and it is denoted by $A_E(F)$.

When $E = \mathbb{C}$ and $F = \mathbb{Q}$, this subfield is denoted by $\overline{\mathbb{Q}}$ and it is called the **field of algebraic numbers over $\mathbb{Q}$**.

The field $\overline{\mathbb{Q}}$ of algebraic numbers over $\mathbb{Q}$ is one of the most important fields that appear in mathematics. By methods well beyond the scope of this module, it can be shown that the field $\overline{\mathbb{Q}}$ has countably many elements and that the degree $[\overline{\mathbb{Q}} : \mathbb{Q}]$ is infinite. Other results about this field play an important role in the relatively recent proof of Fermat's Last Theorem (Book C, Chapter 12, Section 1), which states that there are no non-trivial integral solutions to the equation $x^n + y^n = z^n$ for any $n \geq 3$.

1.3 Transcendental extensions revisited

Theorem 2.31 of Chapter 18 proves that every field F admits an extension containing a transcendental element over F, that is, an element which is not a root of any polynomial with coefficients in F. Recall that if α is a transcendental element over F, then the field $F(\alpha)$ is called a *transcendental extension* of F. We defined transcendental extensions in Definition 2.16 of Chapter 18. We restate the definition here in the following form.

Definition 1.9 *Transcendental extension*

An extension E of a field F is said to be **transcendental** if E contains at least one element that is transcendental over F.

Now if E is a transcendental extension of F, then the degree $[E : F]$ must be infinite, by Theorem 1.3. This necessary condition, however, is not sufficient. For instance, the field $\overline{\mathbb{Q}}$ of complex algebraic numbers has infinite degree over $\mathbb{Q}$, yet $\overline{\mathbb{Q}}$ is an algebraic extension of the field $\mathbb{Q}$.

A proof that a particular element $\alpha \in E$ is transcendental over F, that is, that there is no polynomial over F that has α as one of its roots, is usually hard. On the other hand, the existence of transcendental elements can, in many cases, be established easily by comparing cardinalities. For example, as we have seen, the subfield $\overline{\mathbb{Q}}$ of $\mathbb{C}$ consisting of all algebraic numbers over $\mathbb{Q}$ is countable, while the field $\mathbb{C}$ is uncountable. It follows that there are uncountably many complex numbers that are transcendental over $\mathbb{Q}$.

Theorem 2.30 of Chapter 18 shows that if α is transcendental over F, then $F(\alpha)$ is isomorphic to the field of fractions of $F[x]$. We are going to use this result to construct more examples of transcendental numbers over $\mathbb{Q}$, and, more generally, over any given field.

Theorem 1.10

Let $L(x)$ be the field of fractions of a polynomial ring $L[x]$ over a field L. Suppose that $z \in L(x)$ and $z \notin L$. Then z is transcendental over L.

Proof We know that the field L is embedded into the polynomial ring $L[x]$. From the construction of the field of fractions of an integral domain given in Section 1 of Chapter 17, we also know that $L[x]$ is embedded in the field of fractions $L(x)$. As a result, the field L is embedded into $L(x)$ by identifying any element $c \in L$ with the fraction $\frac{c}{1}$. It follows that an element $\frac{f(x)}{g(x)} \in L(x)$, where $g(x) \neq 0$, belongs to L if, and only if, $f(x) = cg(x)$ for some $c \in L$.

Let $z = \frac{f(x)}{g(x)} \in L(x)$, with $g(x) \neq 0$, and suppose that $z \notin L$. Then $f(x) \neq cg(x)$ for any $c \in L$. (Note that this condition is automatically satisfied if the polynomials $f(x)$ and $g(x)$ do not have the same degree.) We suppose that z is algebraic over L and derive a contradiction from this assumption.

By Theorem 4.2 of Chapter 18, there exists an extension K of L containing all the roots of both $f(x)$ and $g(x)$.

By the solution to Exercise 1.4 of Chapter 17, we can choose polynomials $f_1(x)$ and $g_1(x)$ in $K[x]$ so that $z = \frac{f_1(x)}{g_1(x)}$, and so that the sum of the degrees of $f_1(x)$ and $g_1(x)$ is as small as possible, that is, so that $f_1(x)$ and $g_1(x)$ do not have a common root in K.

Recall that we are assuming that z is algebraic over L. Then, by the solution to Exercise 1.2, the element z is also algebraic over K. By Theorem 2.21 of Chapter 18, this implies that there exists a non-zero irreducible polynomial $h(x)$ in the ring $K[x]$ such that $h(z) = 0$.

Let $h(x) = a_0 + a_1x + \cdots + a_{m-1}x^{m-1} + a_mx^m$, where $a_j \in K$ for all $j \in \{0, 1, \ldots, m\}$ and where $a_m \neq 0$ and $m \geq 1$. Since $h(x)$ is irreducible, we also have that $a_0 \neq 0$.

Substituting $z = \frac{f_1(x)}{g_1(x)}$ in the equation $h(z) = 0$ yields

$$a_0 + a_1\frac{f_1(x)}{g_1(x)} + \cdots + a_{m-1}\left(\frac{f_1(x)}{g_1(x)}\right)^{m-1} + a_m\left(\frac{f_1(x)}{g_1(x)}\right)^m = 0.$$

Multiplying both sides of this equation by $(g_1(x))^m$ removes the denominators and gives the equation

$$\begin{aligned} a_0(g_1(x))^m + a_1f_1(x)(g_1(x))^{m-1} + \cdots \\ + a_{m-1}(f_1(x))^{m-1}g_1(x) + a_m(f_1(x))^m = 0 \end{aligned}$$

in the ring $K[x]$.

By rearranging this equation as

$$\begin{aligned} &a_0(g_1(x))^m \\ &\quad = -(a_1f_1(x)(g_1(x))^{m-1} + \cdots + a_{m-1}(f_1(x))^{m-1}g_1(x) + a_m(f_1(x))^m), \end{aligned}$$

we can see that $f_1(x)$ is a divisor of $(g_1(x))^m$. Similarly, rearranging the equation as

$$\begin{aligned} &a_m(f_1(x))^m \\ &\quad = -(a_0(g_1(x))^m + a_1f_1(x)(g_1(x))^{m-1} + \cdots + a_{m-1}(f_1(x))^{m-1}g_1(x)), \end{aligned}$$

shows that $g_1(x)$ is a divisor of $(f_1(x))^m$.

Since both $f_1(x)$ and $g_1(x)$ have all their roots in K, this implies that $f_1(x)$ and $g_1(x)$ must have the same set of roots. But we chose $f_1(x)$ and $g_1(x)$ not to have common roots. These conclusions can only hold simultaneously if $f_1(x)$ and $g_1(x)$ are both polynomials of degree zero over K, and hence also over L. In particular, the element $z = \frac{f_1(x)}{g_1(x)}$ must then be equal to some $c \in L$. This contradicts our initial assumption on z.

The contradiction arose from supposing that z is algebraic over L, and so we can conclude that z is transcendental over L. ■

One consequence of this result is that in the transcendental extension $\mathbb{Q}(\pi)$, all fractions of the form $\frac{f(\pi)}{g(\pi)}$, where $f(x)$ and $g(x)$ are polynomials with rational coefficients and $g(x)$ is non-zero, are transcendental numbers as long as $f(x)$ is not a rational multiple of $g(x)$. Indeed, by Theorem 1.10, all the elements of $\mathbb{Q}(\pi)$ that are not rational are transcendental numbers.

We conclude this subsection with another way of producing a variety of transcendental numbers. This construction differs from the ones given in Chapter 18 as, given a transcendental element α over a field L, it allows us

to construct transcendental elements outside the extension $L(\alpha)$. We start by establishing some notation.

Let F be a field and suppose that $\alpha \in F$. Then $\sqrt[n]{\alpha^m}$ denotes any root of the polynomial $x^n - \alpha^m$. When working in $\mathbb{C}$ this notation is normally reserved for the principal root, namely the one with smallest non-negative argument. We are not doing this here, since in general we do not have a definition of 'principal' root. This means that the expression $\sqrt[n]{\alpha^m}$ is multi-valued.

Theorem 1.11

Let α be a transcendental element over a field F. Then, for any non-zero relatively prime integers m and n, the element $\sqrt[n]{\alpha^m}$ is transcendental over F.

Proof Let $\beta = \alpha^m$. Then $\beta \in F(\alpha)$. We first show that $\beta = \alpha^m$ is transcendental over F.

Suppose that β is algebraic over F. Then, by Theorem 1.2, $[F(\beta) : F]$ is finite, say equal to n. If m is positive, then $[F(\alpha) : F(\beta)] = m$. Then, by the KLM Theorem (Chapter 18, Theorem 2.29), we have $[F(\alpha) : F] = mn$, which implies that α is algebraic over F, a contradiction. If m is negative, then $\alpha = \beta^{-m} \in F(\beta)$ and so α is not transcendental, a contradiction again. Thus β is transcendental over F.

The element $\sqrt[n]{\beta}$ represents any solution of the equation $x^n = \beta$ and so, by Theorem 4.2 of Chapter 18, it is an element of the splitting field K for the polynomial $x^n - \beta$ over the field $F(\alpha)$.

Suppose that $\sqrt[n]{\beta}$ is algebraic over F. Then, by Theorem 1.5, $(\sqrt[n]{\beta})^n = \beta$ would also be algebraic, contrary to what we have just proved about β. It follows that $\sqrt[n]{\alpha^m}$ is transcendental over F. ■

As a consequence, all the non-zero rational powers of both e and π, for example numbers such as $\sqrt[19]{\pi^{16}}$, are transcendental over $\mathbb{Q}$.

Exercise 1.6

For each of the following elements, decide whether it is algebraic or transcendental over the given field. Briefly justify your decision.

(a) $\sqrt{e}$ over $\mathbb{Q}$

(b) $\sqrt{e}$ over $\mathbb{Q}(e)$

(c) $e^{i\pi}$ over $\mathbb{Q}$

We conclude this section with a summary of the various results we have obtained about field extensions.

Summary – Field extensions

Let E be a field with a subfield F.

- An element $\alpha \in E$ is said to be algebraic over F if α is a root of some polynomial in $F[x]$. An element $\alpha \in E$ is called transcendental over F if α is not a root of any non-zero polynomial in $F[x]$. (Definition 2.11 of Chapter 18)
- If $\alpha \in E \backslash F$ is algebraic over F then
  - α has a minimal polynomial $m(x)$ with $m(\alpha) = 0$
  - $F(\alpha) \cong F[x]/\langle m(x) \rangle$
  - $[F(\alpha) : F] = \deg(m)$
  - $F(\alpha) = \{a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} : a_0, a_1, \ldots, a_{n-1} \in F\}$ where $n = \deg(m)$ and addition and multiplication of elements are carried out modulo $m(x)$.

  (Theorem 2.21, Theorem 2.19 and Definition 2.22 of Chapter 18)
- Let K, L and M be fields such that $K \subset L \subset M$ and let the degrees $[M : L]$ and $[L : K]$ be both finite. Then, $[M : L][L : K] = [M : K]$. (Theorem 2.29 of Chapter 18)
- An element α of E is algebraic over F if, and only if, the degree $[F(\alpha) : F]$ is finite. (Theorem 1.2)
- The degree $[E : F]$ is finite if, and only if, E is an algebraic extension of F and there exists a finite subset S of E such that $E = F(S)$. (Theorem 1.3)
- If $h(x)$ is an irreducible polynomial over a field F and α and β are roots of $h(x)$, then $F(\alpha) \cong F(\beta)$. (Exercise 2.5 of Chapter 18)
- If $f(x)$ is a polynomial over F, then up to isomorphism there is a unique extension of F – the splitting field of f – that contains all the roots of f. Moreover, every extension of F over which f splits contains a subfield that is isomorphic to the splitting field. (Definition 4.1, Proposition 4.4 and Corollary 4.7 of Chapter 18)
- Given a field F, the field of rational functions over F is a transcendental extension of F. (Theorem 2.31 of Chapter 18 and Definition 1.9)
- If α, β are transcendental elements over F, then $F(\alpha) \cong F(\beta)$. (Corollary 2.32 of Chapter 18)
- If α is transcendental over F and $\beta \in F(\alpha)$ but $\beta \notin F$ then β is transcendental over F. (Theorem 1.10)
- If α is transcendental over F and m and n are relatively prime integers then $\sqrt[n]{\alpha^m}$ is transcendental over F. (Theorem 1.11)

2 Ruler and compasses constructions

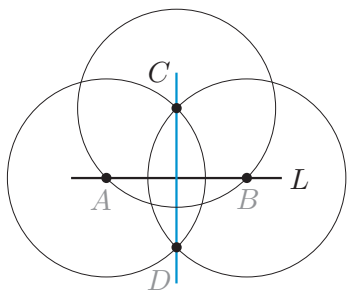
Ruler and compasses constructions are a heritage of the geometry developed by the ancient Greeks. In their view, figures constructed by ruler and compasses wore a stamp of perfection. It was this view that was the driving force behind trying to find ways to construct various objects by using just a ruler (with no marks at all) and compasses.

2.1 Geometric constructions

You may be familiar with a number of simple constructions made with the help of ruler and compasses only. Examples include the construction of a line perpendicular to a given line through a given point (see Figure 2.1 and Figure 2.2) and the construction of a 60° angle (see Figure 2.3). You may wish to try out some of these constructions yourself. You can either do this using paper, pencil, ruler and compasses or you can use readily available software on the web or mobile apps that enable you to simulate constructions on screen.

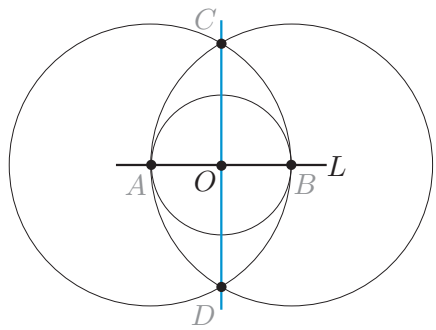
In the examples that follow, we do not list the steps of more basic constructions, such as finding the perpendicular to a given line through a given point, or finding the midpoint of a line segment. You will see these basic constructions in detail in Subsection 2.2.

When we say that we 'construct' an angle, we mean that given a line and a point we can construct a line through that point that makes the required angle with the given line.



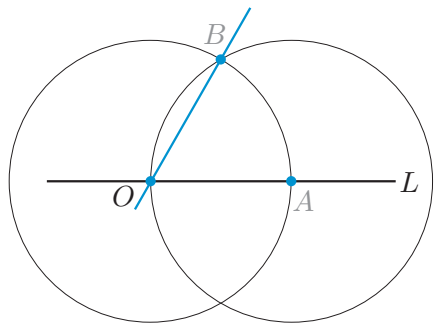
- Given a line L and a point C, draw a circle of centre C cutting L.
- Mark the intersection points with L as A and B.
- Draw two circles with centres A and B and with the same radius as the first circle.
- These circles will intersect at C and another point that we label as D. The line CD passes through C and is perpendicular to the line L.

Figure 2.1 To draw a line perpendicular to a given line L through a given point C



- Given a line L and a point O on L, draw a circle with centre O.
- Mark the intersection points with L as A and B.
- Draw circles, centres A and B, with radius AB.
- Mark the intersection points of these two circles as C and D. CD is a line through O and perpendicular to the line L.

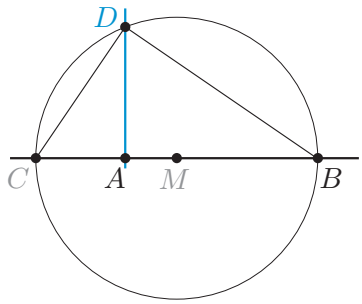
Figure 2.2 To draw a line perpendicular to a given line L through a given point O on L



- Given a line L, mark two distinct points O and A on L.
- Draw a circle of centre O and radius OA.
- Draw a circle of centre A and radius OA.
- These circles will intersect at a point that we label as B. Then the line through O and B is at angle $60°$ to the line L.

Figure 2.3 To draw an angle of $60°$

Another interesting construction is that of the square root of a given length. This is illustrated in Figure 2.4 below, where we assume that we are given both a length 1 and the length whose root is to be determined.



To draw a line whose length is the square root of the given length AB:

- extend the line AB to CB so that $AC = 1$
- find the midpoint M of the line CB (see Exercise 2.1)
- draw the circle of centre M and radius MB
- draw the perpendicular to AB at A, and mark the intersection point with the circle as D
- the length AD is the square root of the length AB, since $\frac{AD}{AC} = \frac{AB}{AD}$ and $(AD)^2 = AC \cdot AB$ so that $(AD)^2 = AB$ as $AC = 1$.

Figure 2.4 Constructing a square root

We mention another famous example without illustrating it: given a construction for a square of a given side, say of length x, we can draw its diagonal, which has length $\sqrt{2}x$. Then the construction can be applied to the diagonal, giving a square whose area is twice the area of the original square.

A construction of a similar flavour is that of a square whose area is equal to the area of a given rectangle. This construction is shown in Figure 2.5 and the steps are given below.

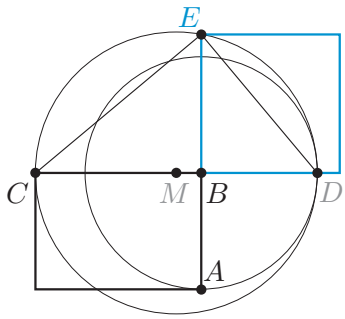


Figure 2.5 Constructing a square with the same area as a given rectangle

Start with the rectangle with vertices at A, B and C.

- Extend the line CB to the right.
- Draw a circle of centre B and radius AB.
- Mark the intersection of the circle with CB, to the right of B, as D.
- Find the midpoint M of the line CD.
- Draw a circle of centre M and radius MD.
- Mark the intersection of this circle with the extended line AB as E.
- Draw a square with side BE.
- The area of the square is the same as that of the rectangle.
- The triangle CBE is similar to the triangle EBD, so $\frac{BC}{EB} = \frac{EB}{BD} = \frac{EB}{AB}$ and therefore $(EB)^2 = BC \cdot AB$.

A large number of other interesting examples exist. There are, however, a number of problems in plane and space geometry that cannot be solved by ruler and compasses only. The three famous problems of this kind which ancient Greeks tried to solve by ruler and compasses but without success were the duplication of a cube, the trisection of an angle, and the quadrature of a circle. The problems ask for a ruler and compasses construction of the side of a cube twice the volume of a given cube, an angle one-third the size of a given angle, and the side of a square of area equal to the area of a given circle, respectively.

You may have come across these three classical problems before because they frequently appear in articles and programs about mathematics for the general public. Our aim in this section is to give rigorous proofs of the impossibility of solving them by ruler and compasses only. The key is to couple geometry with algebra by first using coordinates to translate the geometric nature of the problems into algebraic terms and then apply the theory of field extensions developed in Chapter 18 and in this chapter. This, of course, was not known to ancient Greeks, who apparently did not even have suspicions about possible non-existence of solutions.

2.2 Ruler and compasses algebraically

This subsection develops an algebraic description of the rather intuitive concept of a construction by means of ruler and compasses only. You might have observed that in all the constructions discussed in Subsection 2.1, including the 'impossible' ones, we assume that an initial set of points is given, and out of this 'input set' we construct, using ruler and compasses only, an 'output set' of points that, in one way or another, tells us what the solution is.

A formal description of constructions by ruler and compasses may thus be given as follows.

Definition 2.1 Constructible sets of points

Let S be a set of points in the Euclidean plane that contains at least two points. We introduce two operations corresponding to performing an elementary 'move' using ruler and compasses:

O1 Ruler operation Draw a straight line through any two points of S.

O2 Compasses operation Draw a circle whose centre is a point of S and whose radius is equal to the distance between some pair of points in S.

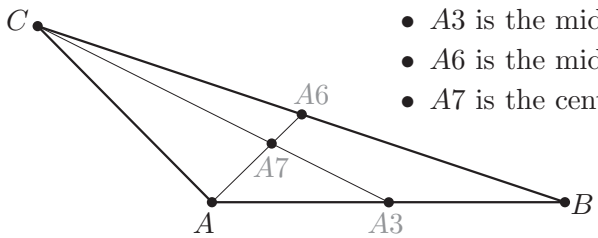
The points of intersection of any two distinct lines or circles drawn using operations O1 or O2 are said to be **constructible from a set** S in one move.

We say that a point B is **constructible** from an initial set S_0 of points in the Euclidean plane if there is a finite sequence $A_1, A_2, \ldots, A_k = B$ of points in the plane such that, for $i = 1, 2, \ldots, k$, the point A_i is constructible in one move from the set $S_0 \cup \{A_1, \ldots, A_{i-1}\}$.

We illustrate this formal definition of constructibility on the example of finding the centroid of a triangle ABC, that is, the point of intersection of the three medians of the triangle. The idea is to bisect the segments AB and BC; the centroid then lies on the intersection of the line through C and the midpoint of the segment AB and the line through A and the midpoint of BC, as shown in Figure 2.6.

Remember that a median is a line connecting one vertex of the triangle with the midpoint of the opposite side.

The construction lines for the midpoints have been omitted.



- $A3$ is the midpoint of AB.
- $A6$ is the midpoint of BC.
- $A7$ is the centroid.

Figure 2.6 Constructing the centroid of a triangle

Example 2.2 *The centroid of a triangle*

We may assume that we are given the three vertices A, B and C of a triangle. Thus, our 'input set' will be $S_0 = \{A, B, C\}$.

1. Draw the circle centred at A of radius AB. (O2)
2. Draw the circle centred at B of radius AB. (O2)
3. Let A_1 and A_2 be the points of intersection of the two circles.
4. Draw the line through A_1 and A_2. (O1)
5. Let A_3 be the point of intersection of the lines through A_1, A_2 and through A, B.
6. Draw the circle centred at B of radius BC. (O2)
7. Draw the circle centred at C of radius BC. (O2)
8. Let A_4 and A_5 be the points of intersection of the two circles.
9. Draw the line through A_4 and A_5. (O1)
10. Let A_6 be the point of intersection of the lines through A_4, A_5 and through B, C.
11. Draw the line through C and A_3. (O1)
12. Draw the line through A and A_6. (O1)
13. Let A_7 be the point of intersection of the last two lines. This point is the centroid of the triangle.

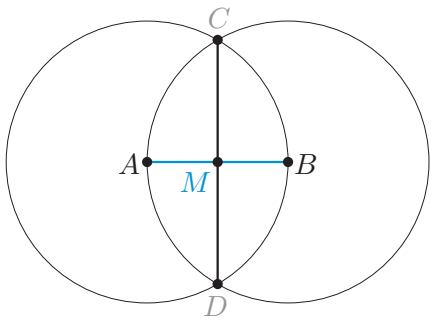
In our terminology, the sequence $A_1, A_2, A_3, A_4, A_5, A_6, A_7$ defines a construction of the centroid of the triangle ABC from the input set $\{A, B, C\}$. Figure 2.6 shows some of the details of this construction.

Our formal definition of constructibility indeed captures all the ruler and compasses constructions we have met in Euclidean geometry. This is because to draw a line requires two specified points on the line, and to draw a circle requires having its centre and radius, these being again given by two specified points (the centre and a point on the circumference).

Exercise 2.1

Describe the process of drawing the midpoint of a segment given its two endpoints in the same way as in Example 2.2, that is, label each operation in the process as O1 or O2. Figure 2.7 shows the standard construction for a midpoint.

For this exercise you should assume that the compass collapses when lifted off the page and so cannot be used to 'transfer' distance.

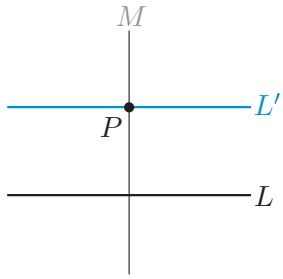


- With centre A, draw a circle of radius AB.
- With centre B, draw a circle of radius AB.
- Label the two intersections of the circles as C and D.
- The line CD is the perpendicular bisector to AB.
- The midpoint M is the intersection of CD and AB.

Figure 2.7 Finding the midpoint of a segment of given endpoints

Exercise 2.2

Describe the process of drawing a line parallel to another line L through a given point P in the same way as in Example 2.2, that is, label each operation as O1 or O2. Figure 2.8 gives a standard construction that involves drawing a perpendicular, M, to L through P. The line through P and perpendicular to M is then the required parallel.



- The line L and the point P are given.
- Draw the perpendicular, M, from P to L.
- Draw the perpendicular to M at P.
- Then L' is the line through P, parallel to L.

Figure 2.8 To draw a line through a point P parallel to another line

Exercise 2.3

Describe how to draw a circle with centre C and radius equal to AB given three points A, B and C not all lying on the same line. You may use the construction of a parallel line described in Exercise 2.2.

The solution to Exercise 2.3 shows that we can

- copy a length, that is, given a line segment AB and point C on a line L we can construct a point D on L so that AB and CD have the same length;
- always draw a circle of radius 1, since an input set S will always contain two points and these can be labelled as $(0,0),(1,0)$.

Exercise 2.4

Given two lines meeting at a point V and another line with a point A, describe how to draw a line through A so that the angle made by the lines meeting at A is the same as the angle between the two lines meeting at V (you may assume that you can copy a length and draw a circle of radius 1).

At this point it is worth collecting some standard constructions that we can incorporate into descriptions without giving full details.

C1 Copy a length.

C2 Draw a circle of radius 1.

C3 Draw a line through the origin at 60° (see Figure 2.3).

C4 Draw a perpendicular to a line through a given point.

C5 Find the midpoint of two points.

C6 Draw a line parallel to a given line through a point not on the given line.

C7 Copy an angle.

Exercise 2.5

Describe the following constructions using the operations O1 and O2 and the constructions C1–C7.

(a) Given a point $(a,0)$, construct the points $(\frac{a}{3},0)$ and $(\frac{2a}{3},0)$.

(b) Divide the line between $(0,0)$ and $(a,0)$ into n equal parts.

(c) Construct the tangent to a circle from a given point not on the circle.

(d) Given two circles with different radii and one not inside the other, construct the two common external tangents as shown in Figure 2.9.

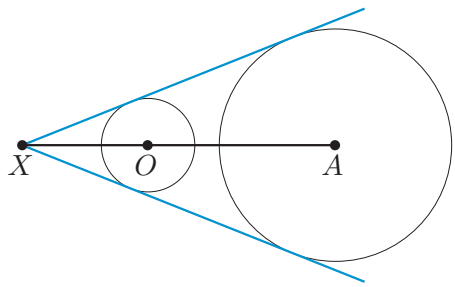


Figure 2.9

Hint: for part (d), use the fact that a tangent is perpendicular to a radius so that the radii that meet the tangent in the two circles are parallel. Then use some similar triangles to locate the point X on the diagram. Finally, use the fact that the angle subtended on the circumference by a diameter is a right angle.

2.3 Coordinates and field extensions

Recall that our formal construction resulted in a sequence $A_1, A_2, \ldots, A_k$ of points obtained from an initial set S_0 of points. We now extend this idea to sequences and sets of real numbers.

Definition 2.3 *Constructible number*

(a) We say that a real number a is **constructible** if the point $(a, 0)$ is constructible from the set of points $\{(0, 0), (1, 0)\}$.

(b) Let S be a set of points in the plane that contains at least two points. We first determine a coordinate system. Choose two points in S and let one point be the origin, $(0, 0)$ and the other point be the point $(1, 0)$. We say that a real number a is **constructible from a set** S, with the given coordinate system, if the point $(a, 0)$ is constructible from the set of points S.

We first show that a set of constructible numbers forms a field.

Proposition 2.4

The set of constructible numbers from a set S containing at least two points forms a subfield of $\mathbb{R}$.

Proof We prove the theorem by showing that if a, b are non-zero constructible numbers from a set S, then the numbers $-a$, $a + b$, ab and $\frac{a}{b}$ are constructible as well. We first note that our definition of constructible points and numbers tells us that the points $O = (0, 0)$ and $I = (1, 0)$ (and hence the numbers 0 and 1) are constructible. The line through these points is the x-axis.

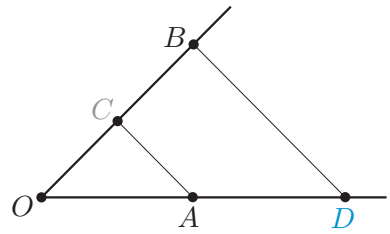
Let a, b be constructible, so that the points $A = (a, 0)$ and $B = (b, 0)$ are constructible. Firstly, draw a circle centred at O through A. The point $(-a, 0)$ is the intersection of this circle with the line AB that is not A, which implies that $-a$ is constructible.

To demonstrate the constructibility of $a + b$ we assume without loss of generality that $b > a > 0$. The construction is as follows.

1. Draw the circle centred at B with radius a. (O2)
2. This circle intersects the line through O and B in two points; mark the one lying outside the segment OB as $C = (a + b, 0)$.

This shows that $(a + b, 0)$ is constructible.

Figure 2.10 shows the construction of $(ab, 0)$ for $a, b > 0$. The construction lines for the parallel lines have been omitted.



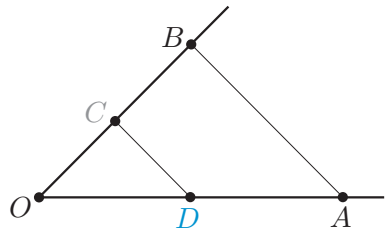
- OA has length a.
- OC has length 1 and OB has length b.
- D is constructed so that BD is parallel to CA.
- Triangle OAC is similar to triangle ODB.
- $\frac{OA}{OC} = \frac{OD}{OB}$ and so $OD = ab$.

Figure 2.10 Constructing ab from a and b

1. Draw the line through the origin O and $A = (a, 0)$. This is the x-axis. (O1)
2. Draw a line, L, through the origin, that does not pass through I $(= (1, 0))$. (O1)
3. Mark points C and B at distance 1 and b from the origin respectively. (C1)
4. Draw the line through A $(= (a, 0))$ and C. (O1)
5. Construct a line through B that is parallel to the line AC. (C6)
6. Mark the intersection of this line with the x-axis as D.

Since triangles OAC and ODB are similar, we have that $\frac{OA}{OC} = \frac{OD}{OB}$ and so $OD = ab$, that is, D is the point $(ab, 0)$.

The construction of $(\frac{a}{b}, 0)$ for $a, b > 0$ is shown in Figure 2.11. As in Figure 2.10, the construction lines for parallel lines have been omitted.



- OA has length a.
- OC has length 1 and OB has length b.
- D is constructed so that CD is parallel to BA.
- Triangle ODC is similar to triangle OAB.
- $\frac{OD}{OC} = \frac{OA}{OB}$ and so $OD = \frac{a}{b}$.

Figure 2.11 Constructing $\frac{a}{b}$ from a and b

1. Draw the line through the origin O and A $(= (a, 0))$. This is the x-axis. (O1)
2. Draw a line, L, through the origin, that does not pass through I $(= (1, 0))$. (O1)
3. Mark points C and B at distance 1 and b from the origin respectively. (C1)
4. Draw the line through A and B. (O1)
5. Construct a line through C that is parallel to the line AB. (C6)
6. Mark the intersection of this line with the x-axis as D.

Since triangles ODC and OAB are similar we have that $\frac{OD}{OC} = \frac{OA}{OB}$ and so $OD = \frac{a}{b}$, that is D is the point $(\frac{a}{b}, 0)$.

We have shown that additive inverses, sums, products and quotients of constructible numbers are constructible. This implies that the set of all the numbers constructible from a given set S containing at least two points is a subfield of $\mathbb{R}$, as claimed. ■

We have shown that the set of constructible points formed from a starting set S is a subfield, K say, of $\mathbb{R}$. We now look at certain subfields of K obtained by adjoining the coordinates of a point constructed from a given set of points in one move.

Lemma 2.5

Let S be a set of at least two points in the plane and let K be the subfield of $\mathbb{R}$ generated by the x- and y-coordinates of the points in S. Let $A = (x, y)$ be a point constructed in one move from the set S and let $L = K(x, y)$ be the subfield of $\mathbb{R}$ obtained by adjoining x and y to K. Then the degree $[L : K]$ is either 1 or 2.

Proof The claim will be verified if we show that x and y are real roots of linear or quadratic polynomials with coefficients in K.

We have to consider three cases, since the point A can arise as an intersection of two lines, a line and a circle, and two non-concentric circles. In each case we make use of the fact that a line in $\mathbb{R}^2$ can be identified with the set of all pairs $(x, y) \in \mathbb{R}^2$ that satisfy a linear equation $ax + by = c$ for some real a, b, c such that $(a, b) \neq (0, 0)$, and a circle can be identified with the set of all pairs $(x, y) \in \mathbb{R}^2$ that satisfy a quadratic equation of the form $(x - s)^2 + (y - t)^2 = r^2$ for some real r, s, t such that $r > 0$.

Suppose first that the point A has been obtained as an intersection of two distinct lines, with equations, say, $a_1x + b_1y = c_1$ and $a_2x + b_2y = c_2$. By our constructibility assumption, both lines have been constructed from points in S, that is, we assume that all the six coefficients belong to K. From elementary algebra we know that the solution is

$$x = \frac{c_1b_2 - c_2b_1}{a_1b_2 - a_2b_1} \quad \text{and} \quad y = \frac{a_1c_2 - a_2c_1}{a_1b_2 - a_2b_1},$$

that is, $x, y \in K$.

Secondly, let A arise as a point of intersection of a line given by the equation $ax + by = c$ with a circle given by $(x - s)^2 + (y - t)^2 = r^2$. By the same token as above, we assume that all the five coefficients a, b, c, s, t are in K. We do not know whether r is an element of K, but since r^2 is a distance of two points with coordinates in K, we definitely know that $r^2 \in K$. We know that $(a, b) \neq (0, 0)$; without loss of generality, assume that $b \neq 0$. Then, out of the equation of the line we have $y = \frac{c-ax}{b}$. Substituting this into the equation of the circle gives

$$(x - s)^2 + \left(\frac{c - ax}{b} - t\right)^2 = r^2,$$

which is a quadratic equation with coefficients in K. Therefore, the coordinates x and y in this case are roots of quadratic polynomials over K and hence $[L : K] \leq 2$, as claimed.

The third and final case to consider is when A arises as a point of intersection of two circles with distinct centres, with equations, say, $(x - s_1)^2 + (y - t_1)^2 = r_1^2$ and $(x - s_2)^2 + (y - t_2)^2 = r_2^2$. Again, we know that $s_1, t_1, s_2, t_2 \in K$ and $r_1^2, r_2^2 \in K$. Since the circles cannot have the same centre it is not possible that $s_1 = s_2$ and $t_1 = t_2$. Expanding the brackets in the two equations gives

$$x^2 + y^2 - 2s_1x - 2t_1y = r_1^2 - s_1^2 - t_1^2,$$
$$x^2 + y^2 - 2s_2x - 2t_2y = r_2^2 - s_2^2 - t_2^2.$$

Subtracting the second equation from the first yields

$$2(s_2 - s_1)x + 2(t_2 - t_1)y = r_1^2 - r_2^2 + s_2^2 - s_1^2 + t_2^2 - t_1^2.$$

Since $s_1 \neq s_2$ or $t_1 \neq t_2$ we can assume, without loss of generality, that $t_1 \neq t_2$. Then we can make y the subject of the third equation and substitute the result into the first. This gives a single quadratic equation for x, with all the coefficients in K. The unknown y is then evaluated from the third equation in terms of x.

Summing up, we have proved that $L = K(x, y)$ arises from K by adjoining real numbers x and y that are roots of linear or quadratic polynomials over K. The result follows. ■

We now derive our main result, a necessary condition for constructibility.

Theorem 2.6

Suppose that the point $A = (x, y)$ is constructible from a set S of at least two points in $\mathbb{R}^2$. Let E be the subfield of $\mathbb{R}$ generated by the coordinates of the points in S. Then the degree $[E(x, y) : E]$ is a power of 2.

Proof Let $A_1, \ldots, A_k = A$ be the finite sequence of points in the plane such that, for $i = 1, 2, \ldots, k$, the point $A_i = (x_i, y_i)$ is constructible in one move from the set $S \cup \{A_1, \ldots, A_{i-1}\}$; note that $(x_k, y_k) = (x, y)$. Further, let $E_0 = E$, and for $i = 1, 2, \ldots, k$ let E_{i-1} be the subfield generated by the x- and y-coordinates of the points in $S \cup \{A_1, \ldots, A_{i-1}\}$.

By Lemma 2.5 applied to the fields $K = E_{i-1}$ and $L = E_i = E_{i-1}(x_i, y_i)$ we see that the degree $[E_i : E_{i-1}]$ is equal to 1 or 2. The KLM Theorem (Chapter 18, Theorem 2.29) then gives

$$[E_k : E_0] = [E_{k-1}(x_k, y_k) : E_{k-1}] \cdots [E_{i-1}(x_i, y_i) : E_{i-1}] \cdots [E_0(x_1, y_1) : E_0]$$

where each term in the product on the right-hand side is 1 or 2. It follows that $[E_k : E_0]$ is a power of 2.

Now $E(x, y) = E_0(x, y)$ is an extension of $E = E_0$ and a subfield of E_k. Thus, $[E(x, y) : E]$ must divide $[E_k : E_0]$ and hence $[E(x, y) : E]$ must be a power of 2. ■

This result will mostly be used is in its contrapositive form, which we state next.

Theorem 2.7

Let S be a set of points in the real plane $\mathbb{R}^2$ and let E be the subfield of $\mathbb{R}$ generated by the coordinates of all the points in S. Suppose that $A = (x, y)$ is a point in $\mathbb{R}^2$ such that the degree of the extension $[E(x, y) : E]$ is not a power of 2. Then the point A is not constructible from S.

We can then use Theorem 2.21(c) of Chapter 18 to state this result in terms of minimal polynomials; for our purposes, it will be sufficient to assume that the point in question lies on the x-axis.

Corollary 2.8

Let S be a set of points in the real plane $\mathbb{R}^2$ and let E be the subfield of $\mathbb{R}$ generated by the coordinates of all the points in S. Let $A = (x, 0)$ be a point in $\mathbb{R}^2$ such that the minimal polynomial for x over the field E has a degree that is not a power of 2. Then x is not a constructible number.

In the next subsection we will apply this result to prove the impossibility of constructing a solution for each of the three classical problems the ancient Greeks could not solve.

Exercise 2.6

Let $S = \{(0, 0), (1, 0)\}$. Why is every point (a, b) with $a, b \in \mathbb{Q}$ constructible?

Exercise 2.7

(a) Show that the perpendicular bisector of the segment with endpoints $A = (1, 2)$ and $B = (3, 4)$ is the line with equation $x + y - 5 = 0$.

(b) Use the equation of the perpendicular bisector found in (a) to find the point of intersection of the line AB and this perpendicular bisector, that is, the midpoint of AB.

2.4 Impossibility proofs for classical Greek problems

We are about to prove that there do not exist any ruler and compasses constructions for three classical problems of Greek geometry: duplication of a cube, trisection of an angle, and quadrature of a circle. Duplicating the cube means constructing a cube of twice the volume of a given cube, and quadrature of the circle is another way of saying squaring the circle, namely, constructing a square of the same area as a given circle.

Theorem 2.9

The cube cannot be duplicated using ruler and compasses only.

Proof Assume that the side of a cube to be duplicated is given. We may assume that the side is placed in the real plane $\mathbb{R}^2$ in such a way that the segment representing it has endpoints with coordinates $A = (0, 0)$ and $B = (1, 0)$ – as this representation only depends on the choice of units on the coordinate axes, our assumption causes no loss of generality. We may therefore assume that our starting set is $\{A, B\}$. Then the smallest subfield of $\mathbb{R}$ containing the coordinates of points in S is $\mathbb{Q}$.

If it were possible to duplicate the cube with ruler and compasses, we would be able to construct the point $(b, 0)$ where $b^3 = 2$, that is, $b = \sqrt[3]{2}$. But as we saw in Example 2.26 of Chapter 18, $[\mathbb{Q}(b) : \mathbb{Q}] = 3$, which is not a power of 2. By Theorem 2.7, such a point is not constructible, and hence duplication of the cube is impossible. ■

Theorem 2.10

The angle $\pi/3$ cannot be trisected by a construction using ruler and compasses only.

Proof We may assume without loss of generality that the angle is given by its vertex $A = (0, 0)$ and two other points $B = (1, 0)$ on the x-axis and $C = (\cos(\pi/3), \sin(\pi/3)) = (\frac{1}{2}, \frac{\sqrt{3}}{2})$ so that the points B, C lie on the unit circle centred at A and BAC is our angle of magnitude $\pi/3$. Note that the point C is actually constructible from A and B and is therefore not necessary (see Figure 2.3).

To trisect the angle $\pi/3$ is then equivalent to constructing the point $D = (d, 0)$ where $d = \cos(\pi/9)$. If D were constructible, then, by doubling the segment AD, we could also construct the point $\Delta = (\delta, 0)$ such that $\delta = 2\cos(\pi/9)$.

At this point we need a formula from trigonometry that can be derived from the formulas for $\cos(\alpha + \beta)$ and $\sin(2\alpha)$:

$$\cos(3\alpha) = 4\cos^3\alpha - 3\cos\alpha.$$

Now, if $\alpha = \pi/9$, we have $\cos(3\alpha) = \frac{1}{2}$, so that our equation multiplied by 2 gives $1 = (2\cos(\pi/9))^3 - 3(2\cos(\pi/9))$. In other words, $\delta = 2\cos(\pi/9)$ is a root of the polynomial $x^3 - 3x - 1$.

By Exercise 2.4 of Chapter 18, however, if α is a root of the polynomial $x^3 - 3x - 1$, then $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$, which is not a power of 2. Theorem 2.7 then tells us that the point Δ is not constructible and therefore the point D is not constructible. This shows the impossibility of trisection of the angle $\pi/3$. ■

Theorem 2.11

The quadrature of a circle cannot be constructed by using ruler and compasses only.

Proof By scaling we may assume that the circle to be 'squared' is the unit circle centred at the origin. The area of this circle is π. Therefore, finding the quadrature of this circle means constructing the point $(\sqrt{\pi}, 0)$ from the origin and the point $(1, 0)$. If this were possible, then the degree $[\mathbb{Q}(\sqrt{\pi}) : \mathbb{Q}]$ would have to be a power of 2. In particular, $\sqrt{\pi}$ and hence π, would have to be algebraic numbers. But a famous theorem by Lindemann, which is beyond the scope of this course, tells us that the number π is not algebraic. This contradiction proves the impossibility of the quadrature of a circle. ■

Exercise 2.8

Can the angle $2\pi/5$ be trisected using ruler and compasses?

Exercise 2.9

Prove that the angle α can be trisected by ruler and compasses if, and only if, the polynomial

$$4x^3 - 3x - \cos(\alpha)$$

is reducible over $\mathbb{Q}(\cos(\alpha))$.

2.5 Constructible complex numbers

The idea of a real constructible number can be extended to a complex number by saying that $a + ib$ is constructible if, and only if, (a, b) is constructible. As i is in a quadratic extension of any subfield of the real numbers (since it is a root of the quadratic polynomial $x^2 + 1$), we can immediately extend our main constructibility result to the complex case.

Theorem 2.12

Let S be a set of complex numbers (including 1 and 0) and let E be the subfield of $\mathbb{C}$ generated by S. Suppose that $a + ib$ is a complex number such that the degree of the extension $[E(a + ib) : E]$ is not a power of 2. Then $a + ib$ is not constructible from S.

We can interpret this theorem in terms of the minimal polynomial of a complex number just as we did for real numbers in Corollary 2.8.

Corollary 2.13

Let K be the field of constructible complex numbers. If the degree of the minimal polynomial for the complex number $a + ib$ over $\mathbb{Q}$ is not a power of 2, then $a + ib \notin K$.

With this result to hand we can combine this with the work on cyclotomic polynomials discussed just before Lemma 4.17 of Book C, Chapter 11, to show that certain roots of unity are not constructible.

Proposition 2.14

Let p be a prime number and let x be a root of $x^p - 1$ with $x \neq 1$. If x is constructible, then p is of the form $2^n + 1$.

Proof Now $x^p - 1 = (x - 1)(x^{p-1} + x^{p-2} + \cdots + x + 1)$, and in Book C, Chapter 11, Worked Exercise 4.18 we showed that $x^{p-1} + x^{p-2} + \cdots + x + 1$ is irreducible when p is prime. Thus $x^{p-1} + x^{p-2} + \cdots + x + 1$ is the minimal polynomial for x, and so if $p - 1$ is not a power of 2, x is not constructible. The result then follows. ■

If we can construct a regular polygon with n sides, we can construct an nth root of unity by making the 'radius' of our polygon 1 and positioning a vertex at $(1, 0)$. Hence if a regular polygon has p sides, where p is a prime number not of the form $2^n + 1$, then it is not constructible. We can see immediately that it is not possible to construct regular polygons with $7, 11$, or 13 sides.

Exercise 2.10

Show that it is impossible to construct a regular 9-gon using ruler and compasses.

Exercise 2.11

This exercise asks you to find two constructions of the regular pentagon.

(a) Let $c = 2\cos\left(\frac{2\pi}{5}\right)$ and let $x = \exp\left(\frac{2i\pi}{5}\right)$, that is, x is a fifth root of unity, so that $x^4 + x^3 + x^2 + x + 1 = 0$. Show that $c = x + \frac{1}{x}$, and hence show that $c^2 + c - 1 = 0$. Deduce that $\cos\left(\frac{2\pi}{5}\right) = \frac{-1+\sqrt{5}}{4}$. Use this to find a construction for the regular pentagon.

(b) This construction is given by Ptolemy in *The Almagest*.

(i) Show that $\cos\left(\frac{\pi}{5}\right) = \frac{1+\sqrt{5}}{4}$.

(ii) Use the cosine rule to show that the length of the side of a decagon, inscribed in a circle of radius 1, has length $\frac{\sqrt{5}-1}{2}$.

(iii) Construct a regular pentagon.

Ptolemy, translated by R. C. Taliaferro, *Almagest I–IV* 'On the size of chords in a circle', pp. 14–15.

Learning outcomes

We list those topics on which we may set assessment questions to test your understanding of the chapter.

After working through this chapter you should be able to:

(a) Find a polynomial equation for an algebraic element over a field in simple cases.

(b) Determine whether a given element of a field extension is transcendental or algebraic in simple cases.

(c) Describe a simple ruler and compasses construction in terms of basic constructions.

(d) Determine whether a given number, point or angle is constructible from a given initial set of points.

(e) Prove simple results about field extensions and ruler and compasses constructions.

Solutions to exercises

Solution to Exercise 1.1

(a) We use the subfield criterion (Book C, Chapter 11, Lemma 1.21) to show that L is a subfield of E. Let $a, b \in L$. If M_i is a subfield of E that contains both S and F then $a, b \in M_i$ and so $a - b \in M_i, ab \in M_i$ and if $b \neq 0$ then $ab^{-1} \in M_i$. Since this is true for all such fields M_i we have $a - b \in L$ and if $b \neq 0$ then $ab^{-1} \in L$. Thus L is a subfield of E.

(b) It is clear that L contains both S and F. If K is another subfield of E that contains both S and F, then L will be a subfield of K since $L = \bigcap M_i$ and $K = M_i$ for some i.

Solution to Exercise 1.2

Since α is algebraic over F there is a polynomial $f(x)$ over F with root $\alpha \in E$. The polynomial $f(x)$ is also a polynomial over K and so α is algebraic over K as required.

Solution to Exercise 1.3

(a) Multiplying numerator and denominator by $1 + \sqrt{2} - (2 + \sqrt{2})\sqrt{3}$ gives the required result.

(b) Since $-15 - 10\sqrt{2} = -5(3 + 2\sqrt{2})$, multiplying the numerator and denominator of $\dfrac{1 + \sqrt{2} - 2\sqrt{3} - \sqrt{6}}{-15 - 10\sqrt{2}}$ by $3 - 2\sqrt{2}$ gives

$$\frac{1}{1 + \sqrt{2} + 2\sqrt{3} + \sqrt{6}} = \frac{1}{5}(1 - \sqrt{2} + 2\sqrt{3} - \sqrt{6}).$$

Solution to Exercise 1.4

(a) From the solution to Worked Exercise 1.4 we know that $\sqrt{2} + \sqrt{3}$ is a root. Since only even powers of x appear in this polynomial, $-\sqrt{2} - \sqrt{3}$ is another root. Again from Worked Exercise 1.4 we have that

$$x^4 - 10x^2 + 1 = (x^2 - (5 + 2\sqrt{6}))(x^2 - (5 - 2\sqrt{6}))$$

and so the other two roots are among the square roots of $5 \pm 2\sqrt{6}$. These square roots can be found by writing out $(a_0 + a_1\sqrt{2} + a_2\sqrt{3} + a_3\sqrt{6})^2$ and comparing coefficients. In our particular case we can bypass the calculation by observing that $(\sqrt{3} - \sqrt{2})^2 = 5 - 2\sqrt{6}$ and so the required roots are $\pm(\sqrt{3} - \sqrt{2})$.

(b) Since $\sqrt{2} + \sqrt{3} \in \mathbb{Q}(\sqrt{2}, \sqrt{3})$ we know that $\mathbb{Q}(\sqrt{2} + \sqrt{3}) \subseteq \mathbb{Q}(\sqrt{2}, \sqrt{3})$. In Exercise 2.10 of Chapter 18 you saw that $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = 4$. We have just shown that $\sqrt{2} + \sqrt{3}$ is a root of an irreducible polynomial of degree 4 over $\mathbb{Q}$, and so $[\mathbb{Q}(\sqrt{2} + \sqrt{3}) : \mathbb{Q}] = 4$. Hence $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$.

(c) Since $\sqrt{2} + \sqrt{3}$ is a root of $x^4 - 10x^2 + 1$, the extension $\mathbb{Q}(\sqrt{2} + \sqrt{3})$ is contained in the splitting field for $x^4 - 10x^2 + 1$.

Now $(\sqrt{2}+\sqrt{3})^2 = 5+2\sqrt{6}$, and so $\sqrt{6} \in \mathbb{Q}(\sqrt{2}+\sqrt{3})$. This implies that $\pm(\sqrt{6}-1) \in \mathbb{Q}(\sqrt{2}+\sqrt{3})$. Thus $x^4 - 10x^2 + 1$ splits over $\mathbb{Q}(\sqrt{2}+\sqrt{3})$ and so $\mathbb{Q}(\sqrt{2}+\sqrt{3})$ is the splitting field for this polynomial.

Solution to Exercise 1.5

(a) In this instance a direct calculation is easiest.

$$\begin{aligned}(1+\sqrt{2})^2 &= 1+2\sqrt{2}+2\\ &= 2(1+\sqrt{2})+1.\end{aligned}$$

Hence a polynomial equation satisfied by $1+\sqrt{2}$ in the field $\mathbb{Q}(\sqrt{2})$ is $x^2 - 2x - 1 = 0$.

(b) Here we use that approach illustrated in Worked Exercise 1.6. A basis for $\mathbb{Q}(\sqrt{2},\sqrt{3})$ is

$$u_1 = 1,\ u_2 = \sqrt{2},\ u_3 = \sqrt{3},\ u_4 = \sqrt{6}.$$

If $\alpha = \sqrt{2} - \sqrt{3}$ we have

$$\begin{aligned}u_1\alpha &= \sqrt{2} - \sqrt{3}\\ u_2\alpha &= 2 - \sqrt{6}\\ u_3\alpha &= \sqrt{6} - 3\\ u_4\alpha &= 2\sqrt{3} - 3\sqrt{2},\end{aligned}$$

so that

$$\begin{aligned}u_1\alpha &= u_2 - u_3\\ u_2\alpha &= 2u_1 - u_4\\ u_3\alpha &= -3u_1 + u_4\\ u_4\alpha &= -3u_2 + 2u_3.\end{aligned}$$

This gives the determinant equation

$$\begin{vmatrix}-\alpha & 1 & -1 & 0\\ 2 & -\alpha & 0 & -1\\ -3 & 0 & -\alpha & 1\\ 0 & -3 & 2 & -\alpha\end{vmatrix} = 0.$$

Swapping columns and multiplying by -1 gives

$$\begin{vmatrix}1 & 0 & \alpha & -1\\ 0 & 1 & -2 & \alpha\\ \alpha & -1 & 3 & 0\\ -2 & \alpha & 0 & 3\end{vmatrix}.$$

Clearing the first column below the diagonal gives:

$$\begin{vmatrix}1 & 0 & \alpha & -1\\ 0 & 1 & -2 & \alpha\\ 0 & -1 & 3-\alpha^2 & \alpha\\ 0 & \alpha & 2\alpha & 1\end{vmatrix} \quad \begin{aligned}r_3 &= r_3 - \alpha r_1\\ r_4 &= r_4 + 2r_1.\end{aligned}$$

Clearing the second column below the diagonal gives

$$\begin{vmatrix} 1 & 0 & \alpha & -1 \\ 0 & 1 & -2 & \alpha \\ 0 & 0 & 1-\alpha^2 & 2\alpha \\ 0 & 0 & 4\alpha & 1-\alpha^2 \end{vmatrix} \quad \begin{matrix} \\ \\ r_3 = r_3 + r_2 \\ r_4 = r_4 - \alpha r_2, \end{matrix}$$

which is equivalent to

$$\begin{vmatrix} 1-\alpha^2 & 2\alpha \\ 4\alpha & 1-\alpha^2 \end{vmatrix} = 0.$$

Evaluating the determinant gives

$$(1-\alpha^2)^2 - 8\alpha^2 = 0$$

and hence

$$\alpha^4 - 10\alpha^2 + 1 = 0.$$

Thus a polynomial equation satisfied by $\sqrt{2} - \sqrt{3}$ in $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ is $x^4 - 10x^2 + 1 = 0$.

Solution to Exercise 1.6

(a) This is transcendental by Theorem 1.11.

(b) This is algebraic over $\mathbb{Q}(e)$ since it is a root of the polynomial $x^2 - e$.

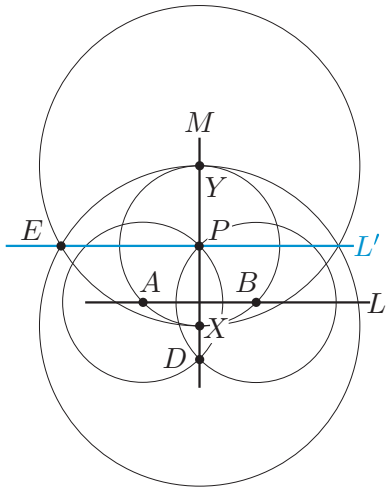
(c) $e^{i\pi} = -1$ and so $e^{i\pi}$ is not transcendental over $\mathbb{Q}$.

Solution to Exercise 2.1

This is in fact the first stage in constructing a centroid so we need the first 5 steps from Example 2.2 with appropriate changes in notation.

1. Draw the circle centred at A of radius AB. (O2)
2. Draw the circle centred at B of radius AB. (O2)
3. Let C and D be the points of intersection of the two circles.
4. Draw the line through C and D. (O1)
5. Let M be the point of intersection of the lines through CD and through AB.

Solution to Exercise 2.2



1. Mark a point A on the line L.
2. Draw a circle C of centre P and radius PA. (O2)
3. Let B be the intersection point of the circle with L that is not A.
4. Draw two circles with centres A and B and radii AP and BP respectively. (O2)
5. Let D be the intersection of the two circles that is not P.
6. Draw the line M through D and P. (O1)
7. Let X and Y be the two intersection points of the circle C with M.
8. Draw two circles with centres X and Y and radius XY. (O2)
9. Let E be an intersection point of the two circles.
10. Draw the line L' through E and P. (O1)

Solution to Exercise 2.3

1. Draw a line parallel to AB through C.
2. Draw a line parallel to AC through B.
3. Mark the intersection of the two lines as D.
4. Draw a circle, centre C and radius CD. (O2)

Since $ABCD$ has been constructed to be a parallelogram, the sides AB and CD will have the same length.

Solution to Exercise 2.4

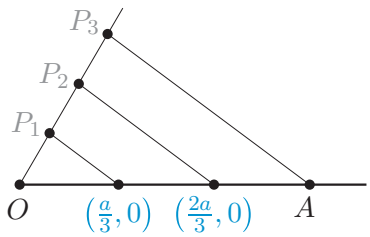
1. Draw circles of radius 1 with centres at V and A respectively.
2. Mark two adjacent intersections of the lines meeting at V with the circle, centre V, as B and C. (The word adjacent is used here since the lines cross at V and give four intersections with the circle.)
3. Mark an intersection of the line through A with the circle of centre A, as D.
4. Draw a circle of centre D and radius BC.
5. Mark an intersection of this circle with the circle of centre A as E.
6. Draw the line AE. (O1)

The angle DAE will be the same as the angle BVC.

Solution to Exercise 2.5

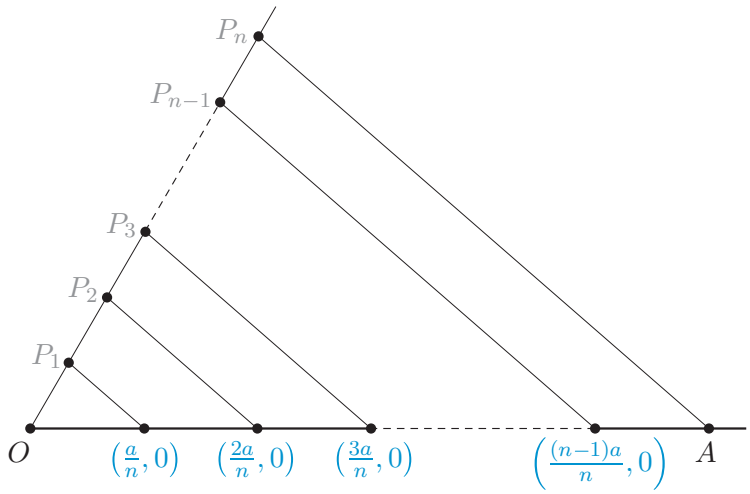
(a) This construction uses the fact that the ratios of corresponding sides of similar triangles are equal.

1. Draw a line through the origin at $60°$. (C3)
2. Mark points P_1, P_2, P_3 along this new line at distance $1, 2, 3$ from the origin respectively. (C1)
3. Draw the line L_3 from P_3 to $(a, 0)$. (O1)
4. Draw L_1 and L_2 parallel to L_3 through P_1 and P_2 respectively. (C6)
5. The intersections of L_1 and L_2 with the x-axis will give the points $(\frac{a}{3}, 0)$ and $(\frac{2a}{3}, 0)$ respectively.



(b) This construction uses the fact that the ratios of corresponding sides of similar triangles are equal.

1. Draw a line through the origin at 60°. (C3)
2. Mark points $P_1, P_2, \ldots, P_n$ at distance $1, 2, \ldots, n$ from the origin respectively. (C1)
3. Draw the line L_n from P_n to $(a, 0)$. (O1)
4. Draw $L_1, L_2, \ldots, L_{n-1}$ parallel to L_n through $P_1, P_2, \ldots, P_{n-1}$ respectively. (C6)
5. The intersections of $L_1, L_2, \ldots, L_{n-1}$ with the x-axis will give the points $(\frac{a}{n}, 0), (\frac{2a}{n}, 0), \ldots, (\frac{(n-1)a}{n}, 0)$ respectively.



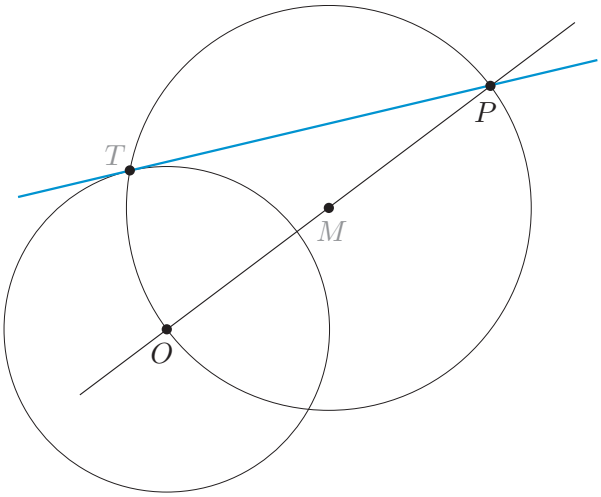
(c) 1. Draw a line between the centre, O, of the circle and the given point, P. (O1)

2. Construct the midpoint, M, of this line. (C5)

3. Draw the circle with centre at this midpoint that passes through the centre of the original circle. (O2)

4. Draw the line from the intersection, T, of the two circles to the given point. (O1)

This last line is a tangent, since it is at right angles to the radius at the intersection point.



(d) 1. Draw the line OA joining the centres of the two circles. (O1)

2. In each circle draw a line through the centre and perpendicular to OA. (C4)

3. Mark the intersections, on one side of OA, of these perpendiculars with the two circles as B and C respectively.

4. Draw the line BC and mark the intersection of this line with OA as X. (O1)

5. Construct the midpoint M of OX. (C5)

6. Construct the midpoint N of XA. (C5)

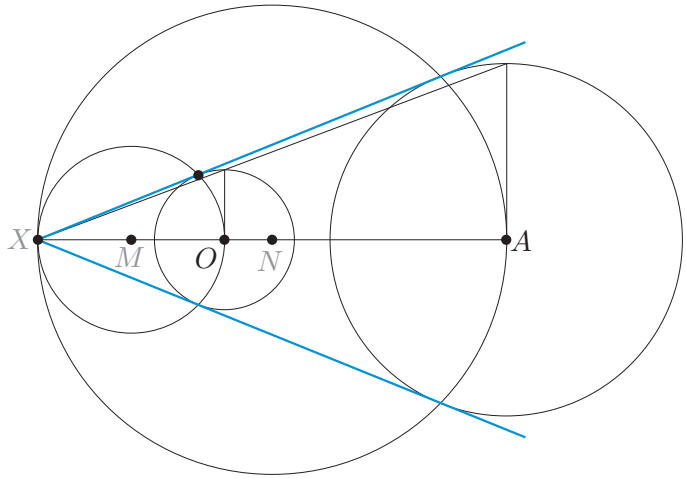
7. Draw the circle through X centre M. (O2)

8. Draw the circle through X centre N. (O2)

9. Mark the intersections of these circles with the original circles.

10. Draw the two lines through X and the two pairs of intersections. (O1)

These two lines will be the required tangents (note that you only need one of the intersections for each tangent).



Solution to Exercise 2.6

Since the set of numbers that are constructible from S is a subfield of $\mathbb{R}$, it must contain $\mathbb{Q}$ by Theorem 1.11 of Chapter 18. The result then follows.

Solution to Exercise 2.7

(a) The perpendicular bisector of AB passes through the points of intersection of the circles:

$$(x-1)^2+(y-2)^2=r^2$$
$$(x-3)^2+(y-4)^2=r^2,$$

where r is the length AB. Subtracting the second equation from the first gives

$$(x-1)^2+(y-2)^2-[(x-3)^2+(y-4)^2]=0\,,$$

which simplifies to $x+y-5=0$.

(b) The line through AB has equation $2(y-2)=2(x-1)$, that is $y-x-1=0$. To find the required point of intersection we need to solve this equation simultaneously with $y+x-5=0$. This gives $x=2, y=3$, as we would expect.

Solution to Exercise 2.8

The trisection of $2\pi/5$ is the angle $2\pi/15$. It is perhaps easier to work using degrees at this stage, so we are asked to construct an angle of $24°$ given an angle of $72°$. This is possible since we can construct an angle of $60°$, which means we can then construct an angle of $12°$. We can double the angle by copying and so construct an angle of $24°$.

Solution to Exercise 2.9

The angle α can be trisected if, and only if, we can construct, over the field $\mathbb{Q}(\cos(\alpha))$, the number $x=\cos\beta$ where $\alpha=3\beta$. Now

$$\cos\alpha=\cos 3\beta=4\cos^3\beta-3\cos\beta,$$

and so x is a root of the polynomial $4x^3-3x-\cos(\alpha)$. If this polynomial is irreducible, then x has a minimal polynomial of degree 3 over $\mathbb{Q}(\cos(\alpha))$, and so cannot be constructed. If it is reducible, it has a linear factor and a quadratic factor. The root of the linear factor is constructible as it is just a linear combination of constructible numbers.

Solution to Exercise 2.10

If it were possible to construct a regular 9-gon with ruler and compasses, then it would be possible to construct an angle of $2\pi/9$ radians. We would then be able to bisect this angle to obtain an angle of $\pi/9$ radians. However, in Theorem 2.10 we showed that this is not possible.

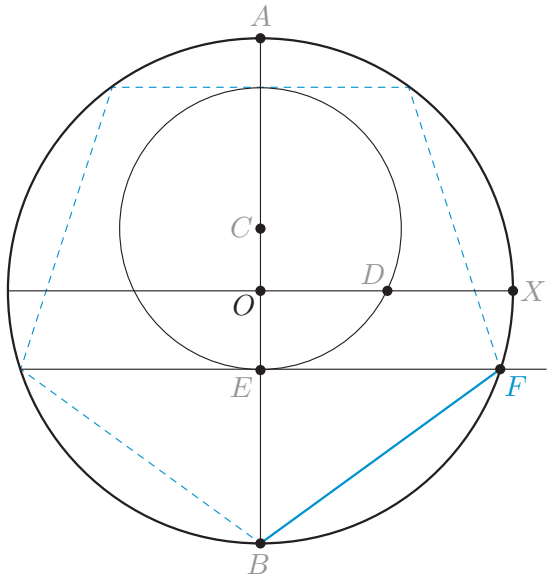
Solution to Exercise 2.11

(a)
$$x = e^{\frac{2i\pi}{5}} = \cos\left(\tfrac{2\pi}{5}\right) + i\sin\left(\tfrac{2\pi}{5}\right)$$
$$\tfrac{1}{x} = e^{-\frac{2i\pi}{5}} = \cos\left(\tfrac{2\pi}{5}\right) - i\sin\left(\tfrac{2\pi}{5}\right)$$
and so $x + \frac{1}{x} = 2\cos\left(\frac{2\pi}{5}\right) = c$, as required.

Now
$$c^2 + c - 1 = \left(x + \frac{1}{x}\right)^2 + x + \frac{1}{x} - 1 = \frac{1}{x^2}[(x^2+1)^2 + x^3 + x - x^2]$$
$$= \frac{1}{x^2}[x^4 + 2x^2 + 1 + x^3 + x - x^2]$$
$$= \frac{1}{x^2}[x^4 + x^3 + x^2 + x + 1].$$

Since $x^4 + x^3 + x^2 + x + 1 = 0$, we have $c^2 + c - 1 = 0$ and so $c = \frac{-1\pm\sqrt{5}}{2}$. Therefore $\cos\left(\frac{2\pi}{5}\right) = \frac{-1+\sqrt{5}}{4}$ since the cosine is positive.

1. Draw a circle of centre O and radius 1, and draw a diameter to that circle. Mark the intersections of the diameter with the circle as A and B.
2. Bisect OA twice so as to find the point C with $OC = \frac{1}{4}$.
3. Draw the diameter XY of the circle perpendicular to AB.
4. Find the midpoint D of OX.
5. Draw a circle of centre C and radius CD ($CD = \frac{\sqrt{5}}{4}$).
6. Mark the intersection of this circle with OB as E.
7. Mark the intersection of the perpendicular to OB at E with the original unit circle as F ($OF = \cos\left(\frac{2\pi}{5}\right)$).
8. BF will be one side of the pentagon.



Constructing a regular pentagon

(b) (i) Suppose that $\cos(\theta) = \frac{1+\sqrt{5}}{4}$.

Then the formula $\cos(2\theta) = 2\cos^2(\theta) - 1$ gives

$$\begin{aligned}\cos\left(\frac{2\pi}{5}\right) &= 2\left(\frac{1+\sqrt{5}}{4}\right)^2 - 1 \\ &= \frac{6+2\sqrt{5}}{8} - 1 \\ &= \frac{-2+2\sqrt{5}}{8} \\ &= \frac{-1+\sqrt{5}}{4}.\end{aligned}$$

The result follows since $\cos\left(\frac{2\pi}{5}\right) = \frac{-1+\sqrt{5}}{4}$.

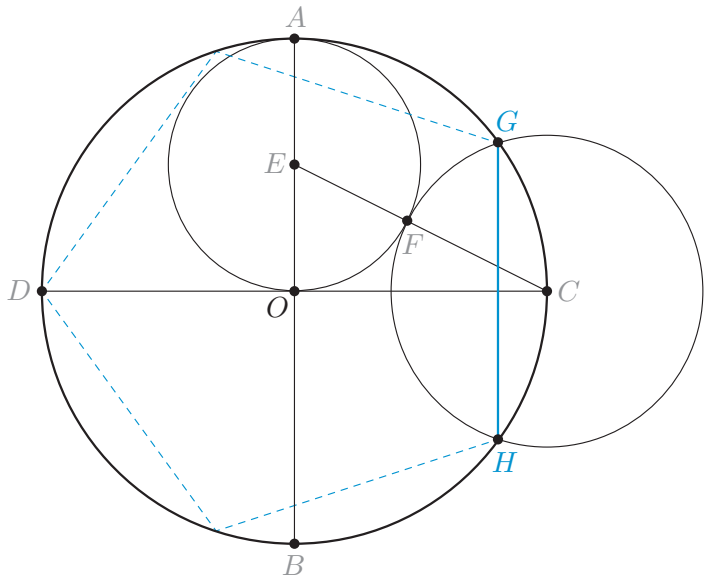
(ii) The length of a side of a decagon will equal the length of the base of an isosceles triangle with equal sides of length 1 enclosing an angle of $\frac{\pi}{5}$. Thus if the length of the base is c, the cosine rule, $c^2 = a^2 + b^2 - 2bc\cos C$, gives

$$\begin{aligned}c^2 &= 2 - 2\frac{1+\sqrt{5}}{4} \\ &= \frac{6-2\sqrt{5}}{4}.\end{aligned}$$

The result follows since $\left(\frac{\sqrt{5}-1}{2}\right)^2 = \frac{6-2\sqrt{5}}{4}$.

(iii) 1. Draw a circle of centre O and radius 1, and draw a diameter to that circle. Mark the intersections of the diameter with the circle as A and B.
2. Draw the diameter CD of the circle perpendicular to AB.
3. Bisect OA so as to find the point E with $OE = \frac{1}{2}$.
4. Draw the line CE, which will have length $CE = \frac{\sqrt{5}}{2}$.
5. Draw the circle of centre E and radius EO, and let it meet CE at F, so $CF = \frac{\sqrt{5}-1}{2}$.
6. Draw the circle of centre C and radius CF, and let it meet the original circle at G.

The side CG is one side of a regular decagon, and the construction of the regular pentagon follows.



A second construction of a regular pentagon

Chapter 20

Public-key cryptography

Introduction

Cryptography may be described as the art of secure real-time communication through an insecure channel, that is, a channel that makes the transmitted message liable to be intercepted by a third party. The way to make the communication secure is to scramble the information through a process known as an **encryption** method. The intended recipient needs to unscramble (**decrypt** or **decipher**) the information on receipt.

Encryption of messages sent by the communicating parties should be fast, that is, real-time. At the same time, encryption should be robust enough that eavesdroppers monitoring the data flow through the channel have no realistic chance to ever decipher the message.

In the context of cryptography, a procedure for implementing a particular method of encryption and decryption is called a **cryptographic system**, or a **cryptosystem**, for short. The history of cryptosystems is long and rich. It ranges from ancient hieroglyphic ciphers (used in the Old Kingdom of Egypt in about 1900 BC) through to simple systems based on alphabet shifting (claimed to have been used by Julius Caesar) and their medieval improvements by Blaise de Vigenère, up to the Enigma code employed by the German military in World War II, to modern cryptosystems to protect communication over the internet.

Before the internet era, cryptosystems relied on a piece of secret information, the **key**, that the sender and the receiver need to share in order to encrypt and decipher the message. For example, the cryptosystem used by Julius Caesar consisted in replacing each letter of the alphabet by the letter that comes three places further down along the alphabet. More generally, any cryptosystem that consists in shifting the alphabet by a given number of places is called a *Caesar cipher*. The key is then the length of the shift, and the cryptosystem assumes that the key is known to the sender for encryption and to the receiver for decryption. The nature of the keys used in Vigenère's system and in the Enigma code was far more complex, and the cryptosystems themselves far more robust than Caesar ciphers, but all of these examples relied on the fact that the key must be known to both the sender and the receiver. This feature is, in fact, a weakness, known as the **key exchange problem**: the key itself is a secret that needs to be exchanged in some form, and it is as liable to being intercepted as the message itself. It took several centuries before anyone questioned the necessity for the sender and the receiver to share the same key. In the mid 1970s, two American mathematicians, Whitfield Diffie and Martin Hellman, began to work on a communication exchange protocol that did not require key exchange: a cryptosystem where the sender uses a key for encryption and the receiver uses another key for decryption. Their intuition that a key exchange could be avoided lies at the basis of what many consider the most powerful breakthrough in the history of cryptography.

In this chapter we will focus precisely on **public-key cryptosystems**. Informally, such systems require two types of key. The two keys, usually in the form of some positive integers, are algebraically linked. One key is used to encrypt a message, often called the **plaintext**, and to produce the corresponding encrypted message, called the **ciphertext**. This key is called a **public key**; anyone who wants to receive a secure communication can generate a public key and make it publicly known, so that anyone who wants to send this recipient a message can encrypt it using this key. The ciphertext is then sent through an agreed channel to the recipient, who decrypts the message using the second key, called a **private key**. The art of secure communication is to devise procedures preventing persons not in possession of the private key (in particular, malicious eavesdroppers monitoring the communication in the channel) to decipher the encrypted message.

It turns out that the procedures used for this purpose are mostly based on certain algebraic techniques that you have encountered earlier in this module: the main ingredients are modular arithmetic and finite fields. Typically, encryption in a public-key cryptosystem is the result of some algebraic operations carried out on the plaintext, suitably coded as a string of numbers. In order to decrypt, one could, in principle, apply the corresponding inverse operations. The encryption procedure, however, is devised in such a way that it is infeasible to find the inverse algebraic operations in real time (in fact, in the lifetime of our universe if one wants an extremely high level of security) without the knowledge of a private key.

Among a variety of public-key cryptosystems that have been proposed in the literature, we will present a sample of four. In Section 1 we introduce two systems based on modular arithmetic, the Rivest–Shamir–Adleman (RSA) system and the Diffie–Hellman system. Section 2 is devoted to cryptosystems based on finite elliptic curves, which can be viewed as abelian groups defined by means of polynomials in two variables over finite fields. Since elliptic curves over more general fields have played an important role in the development of mathematics in the last two centuries, we have included a more detailed introduction to this topic. This chapter concludes with a description of two cryptosystems based on finite elliptic curves, the Diffie–Hellman–ElGamal and the Menezes–Vanstone elliptic cryptosystems.

Chapter guide

This chapter makes considerable use of results obtained earlier in the module as well as in this book. In particular you may find it useful to have Book C readily available for reference. Many of the exercises involve practising numerical techniques, so you may find it helpful to have a simple calculator to hand. For some of the calculations involving elliptic curves, a spreadsheet or other means of evaluating a formula for several inputs would be useful. Note that throughout this chapter GF_p will denote the finite field of p elements, as this avoids confusion with the abelian group $(\mathbb{Z}_p, +)$.

We expect the two sections to require similar amounts of study time.

1 Cryptosystems based on modular arithmetic

This section discusses in some detail two cryptosystems based on modular arithmetic, and, more exactly, on calculations of powers modulo a given positive integer. The two systems we introduce are the RSA and the Diffie–Hellman public-key cryptosystems.

The RSA public-key cryptosystem is named after Ron Rivest, Adi Shamir and Leonard Adleman, who first published the corresponding procedure in 1977. It should be noted that the English mathematician Clifford Cocks discovered an equivalent system in 1973, but this discovery remained classified until 1997.

The RSA system and its variations use a public key that includes a number obtained as a product of two distinct large prime numbers, and its security relies on the fact that the prime factors are kept secret. The algebraic operations that give the encryption use this product, along with other information. The inverse operations needed for decryption turn out to be infeasible in a realistic amount of time unless one knows the two prime factors. Since factorisation of large numbers appears to be an intractable problem, in general RSA systems are regarded as secure.

The second system presented in this section is the Diffie–Hellman public-key cryptosystem. It was first published by Whitfield Diffie and Martin Hellman in 1976. Its story is similar to that of RSA, in that an equivalent system was invented a few years earlier in the UK by Malcolm J. Williamson but was kept classified. The infeasibility of breaking the Diffie–Hellman system relies on a different hard mathematical problem, called the *discrete logarithm problem*.

Subsection 1.1 introduces a few mathematical preliminaries related to modular arithmetic. Subsection 1.2 presents the RSA encryption and decryption schemes (that is, an RSA cryptosystem), followed by two examples in Subsection 1.3. Subsection 1.4 discusses the security of our RSA cryptosystem in some detail and Subsection 1.5 discusses the Diffie–Hellman cryptosystem.

1.1 Algebraic preliminaries

We begin by refreshing your skills in determining the highest common factor of two positive integers. You will recall that this was done in Book A, Chapter 1, Section 5.1 by means of the Euclidean Algorithm. This can be presented as follows.

To determine the highest common factor of two integers a, b such that $2 \leq b < a$, the Euclidean Algorithm proceeds in a series of steps S_i for $i \geq 0$. In order to match our notation with that used in Book A, Chapter 1, we let $r_{-1} = a$ and $r_0 = b$. The input at step S_i is an ordered pair of integers (r_{i-1}, r_i) with $0 < r_i < r_{i-1}$, and the output at S_i is an ordered pair of integers of the form (r_i, r_{i+1}); this output is, at the same time, the input for the next step, S_{i+1}. The body of step S_i consists in performing the Division Algorithm on the pair (r_{i-1}, r_i), that is, in determining the unique positive integer q and the unique integer r_{i+1} such that $0 \leq r_{i+1} < r_i$ and $r_{i-1} = q \times r_i + r_{i+1}$. The output at S_i is the ordered pair consisting of the number we divide by (r_i) and the remainder (r_{i+1}). The process terminates at step S_n if $r_{n+1} = 0$. In summary, the steps are as follows.

The input at step S_0 is the initial pair (a, b), because $a = r_{-1}$ and $b = r_0$.

Step	Input	Division Algorithm	
S_0	(a, b)	$a = q_1 \times b + r_1$	$0 < r_1 < b$
S_1	(b, r_1)	$b = q_2 \times r_1 + r_2$	$0 < r_2 < r_1$
S_2	(r_1, r_2)	$r_1 = q_3 \times r_2 + r_3$	$0 < r_3 < r_2$
$\vdots$	$\vdots$	$\vdots$	$\vdots$
S_i	(r_{i-1}, r_i)	$r_{i-1} = q_{i+1} \times r_i + r_{i+1}$	$0 < r_{i+1} < r_i$
$\vdots$	$\vdots$	$\vdots$	$\vdots$
S_n	(r_{n-1}, r_n)	$r_{n-1} = q_{n+1} \times r_n + 0$	$r_{n+1} = 0$

We now introduce a variant of this procedure which we will call the **Fast Euclidean Algorithm**. It differs from the Euclidean Algorithm as presented above because it requires pre-checking the input at each step. If the input has the form (r_{i-1}, r_i) and $1 < r_i \leq \frac{r_{i-1}}{2}$, step S_i is as above. However, if $r_i > \frac{r_{i-1}}{2}$ we replace r_i with $r_{i-1} - r_i$. and then run step S_i for this new value of r_i. So the Fast Euclidean Algorithm works exactly like the ordinary Euclidean Algorithm, except that pre-checks on the input are needed at each step, as described.

The validity of the Fast Euclidean Algorithm is proved in the same way as the validity of the standard Euclidean Algorithm, using the argument given in Book A, Chapter 1, Section 1.5 together with the fact that $\mathrm{hcf}(r, s) = \mathrm{hcf}(r, r - s)$ for any two positive integers r, s such that $s < r$. You are asked to prove this fact in the next exercise.

Exercise 1.1

Let r and s be two positive integers such that $s < r$. Prove that

$$\mathrm{hcf}(r, s) = \mathrm{hcf}(r, r - s).$$

The next worked exercise illustrates the Fast Euclidean Algorithm.

Worked Exercise 1.1 *Fast Euclidean Algorithm*

Determine the highest common factor of 257 and 151 with the help of the Fast Euclidean Algorithm.

Solution

Running the standard Euclidean Algorithm to determine $\mathrm{hcf}(257, 151)$ would begin by writing

$$257 = 1 \times 151 + 106.$$

The Fast Euclidean Algorithm, however, requires pre-checking the inputs at each step. Here, since $151 > \frac{257}{2}$, we replace 151 with the difference $257 - 151 = 106$ and take the pair $(257, 106)$ as input for the step S_0. In the computation below this pre-check is done at each step S_i, $i \geq 1$. For easier reading, the entries r_i are underlined once and the remainders r_{i+1} twice.

$$\begin{array}{lrcll} S_0\colon & 257 & = & 2 \times \underline{106} + \underline{\underline{45}} & \text{use } \underline{45} \text{ in } S_1, \text{ as } 45 < \frac{106}{2} \\ S_1\colon & 106 & = & 2 \times \underline{45} + \underline{\underline{16}} & \text{use } \underline{16} \text{ in } S_2, \text{ as } 16 < \frac{45}{2} \\ S_2\colon & 45 & = & 2 \times \underline{16} + \underline{\underline{13}} & \text{use } \underline{3} = 16 - 13 \text{ in } S_3, \text{ as } 13 > \frac{16}{2} \\ S_3\colon & 16 & = & 5 \times \underline{3} + \underline{\underline{1}} & \end{array}$$

Since the remainder in the last step is 1, we may terminate the procedure already at this step and conclude that $\mathrm{hcf}(257, 151) = 1$.

Exercise 1.2

Determine the highest common factor of 91 919 and 19 191 with the help of the Fast Euclidean Algorithm.

As our next revision item, we determine the multiplicative inverse of a given number modulo a given integer. Recall from Theorem 3.4(b) of Book A, Chapter 3, that given two positive integers k and e such that $1 \leq e < k$ and e is coprime to k, there exists a unique positive integer d such that $1 \leq d < k$ and $de \equiv 1 \pmod{k}$. The residue class of d modulo k is precisely the multiplicative inverse of the residue class e modulo k in the ring $(\mathbb{Z}_k, +, \times)$. To simplify the explanation, we will simply say that d is the multiplicative inverse of e modulo k.

In the next worked exercise, we will use the Fast Euclidean Algorithm to determine a multiplicative inverse modulo 257. The method is the one employed in Book A, Chapter 1, Worked Exercise 5.2, where we used the equations in the Euclidean Algorithm in reverse order, except that here we use the equations in the Fast Euclidean Algorithm.

Worked Exercise 1.2 *Multiplicative inverses with the Fast Euclidean Algorithm*

Determine the multiplicative inverse of 151 modulo 257 by reversing the Fast Euclidean Algorithm.

Solution

By the result of Worked Exercise 1.1, we know that the multiplicative inverse to 151 modulo 257 indeed exists. (The alert reader may have realised that this is automatic since 257 is a prime!) We determine the multiplicative inverse by taking the last equation in Worked Exercise 1.1 – the one in step S_3 – and working backwards as in the solution to Worked Exercise 5.2 of Book A, Chapter 1. We will need to take into account the replacements in the Fast Euclidean Algorithm.

We begin by writing the equation in step S_3 in the form

$$1 = 16 - 3 \times 5.$$

We continue by making the 'back substitution' $3 = 16 - 13$ and then we substitute for 13 by isolating the doubly underlined 13 from the equation for S_2. We then rearrange terms so that we end up with 1 expressed as a linear combination of the numbers 13 and 16. We continue to step back through the system of equations until we eventually obtain 1 as a linear combination of 151 and 257. The full working is given below, where 'back substitutions' resulting from a replacement have been underlined for clarity.

$$\begin{aligned}
1 &= 16 - 3 \times 5 = 16 - \underline{(16 - 13)} \times 5 \\
&= 16 \times (-4) + 13 \times 5 \\
&= 16 \times (-4) + (45 - 16 \times 2) \times 5 \\
&= 45 \times 5 + 16 \times (-14) \\
&= 45 \times 5 + (106 - 45 \times 2) \times (-14) \\
&= 106 \times (-14) + 45 \times 33 \\
&= 106 \times (-14) + (257 - 106 \times 2) \times 33 \\
&= 257 \times 33 + 106 \times (-80) = 257 \times 33 + \underline{(257 - 151)} \times (-80) \\
&= 257 \times (-47) + 151 \times 80
\end{aligned}$$

We find that $1 = 257 \times (-47) + 151 \times 80$, which gives

$$151 \times 80 \equiv 1 \pmod{257}.$$

This means that the multiplicative inverse of 151 modulo 257 is 80.

Exercise 1.3

Determine the multiplicative inverse to 19 191 modulo 91 919 by reversing the Fast Euclidean Algorithm.

There is an important lesson to be learned from Worked Exercise 1.2 and Exercise 1.3: if r and s are positive and relatively prime integers such that $1 < r < s$, a multiplicative inverse of r modulo s can be determined quickly. Indeed, when running the Fast Euclidean Algorithm, at each step we made sure that the divisor was never larger than half the dividend. It follows that the number of operations needed to express 1 as a linear combination of r and s using the Fast Euclidean Algorithm takes no more than $\text{int}(\log_2 s)$ divisions, where $\text{int}(x)$ denotes the largest integer that does not exceed x. This is because if $\log_2 s = q$, then $2^q = s$, so we can successively divide s by 2 at most $\text{int}(q)$ times before we obtain 1. Note that in our two worked exercises $\text{int}(\log_2 257) = 8$, but only four divisions were needed.

The power of the Fast Euclidean Algorithm becomes more apparent if you think about multiplicative inverses modulo s when the binary expansion of s requires more than 1000 digits. Such numbers are at least as large as 2^{1000}, which, by the way, is much larger than the estimated number of elementary particles in our universe. Yet determining the multiplicative inverse of any given number relatively prime to s with the Fast Euclidean Algorithm would require no more than 1000 divisions!

We will now prove with an auxiliary result from number theory which is closely related to multiplicative inverses. In Book C, Chapter 9, Subsection 3.1 you encountered Euler's ϕ-function: recall that for an integer n, $\phi(n)$ is the number of positive integers smaller than n and relatively prime to n. In Subsection 4.2 of the same chapter you also learned that if n has a prime factorisation of the form

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_t^{\alpha_t},$$

where p_i $(1 \leq i \leq t)$ are the distinct prime factors of n, then

$$\phi(n) = n(1 - p_1^{-1})(1 - p_2^{-1}) \cdots (1 - p_t^{-1}).$$

In what follows, we will need to work with positive integers n that are products of just two distinct primes, that is, with integers of the form $n = pq$, where p and q are prime numbers and $p \neq q$. Observe that our formula for Euler's ϕ-function applied to $n = pq$ yields

$$\phi(n) = (p - 1)(q - 1).$$

For integers n of this kind we now prove a useful result about multiplicative inverses modulo $\phi(n)$.

Lemma 1.3

Let $n = pq$, where p and q are distinct prime numbers, and let e be an integer such that $1 \leq e < \phi(n)$ and e is relatively prime to $\phi(n)$. If d is the multiplicative inverse of e modulo $\phi(n)$, then

$$x^{de} \equiv x \pmod{n}$$

for all integers x.

Proof Since we are working modulo n, it is sufficient to consider the integers x such that $1 \leq x \leq n-1$. The assumption that d is the multiplicative inverse of e is equivalent to $de \equiv 1 \bmod \phi(n)$, which implies that $de = t\phi(n) + 1$ for some integer t.

If p divides x, then $x^{\phi(n)} \equiv x \,(\text{mod } p)$, since both sides of the congruence are equivalent to $0 \,(\text{mod } p)$. If p does not divide x, Fermat's Little Theorem (Book A, Chapter 4, Theorem 1.1) gives $x^{p-1} \equiv 1 \,(\text{mod } p)$, and so

$$x^{(p-1)(q-1)} \equiv 1 \pmod{p},$$

that is $x^{\phi(n)} \equiv 1 \,(\text{mod } p)$. Similarly, we have that $x^{\phi(n)} \equiv 1 \,(\text{mod } q)$. This implies that both p and q divide $x^{\phi(n)} - 1$. But since p and q are primes, the product $pq = n$ also divides $x^{\phi(n)} - 1$ and so $x^{\phi(n)} \equiv 1 \,(\text{mod } n)$. Taking the tth power of this congruence and then multiplying by x gives

$$x^{t\phi(n)+1} \equiv x \pmod{n},$$

or, equivalently, $x^{de} \equiv x \,(\text{mod } n)$. ■

Exercise 1.4

Prove that $x^{841} \equiv x \,(\text{mod } 899)$ for all integers x.

In the next lemma we prove one more fact about congruences that will be helpful later. This fact is, at the same time, another nice application of Fermat's Little Theorem.

For the proof we need to introduce some terminology that will also be useful later: a non-zero element b of GF_p, the finite field of p elements, is said to be a **square** if there exists an $x \in GF_p$ such that $b = x^2$; such an x is said to be a **square root** of b modulo p. Equivalently, if ξ is any primitive element of GF_p, that is, a generator of the multiplicative group of GF_p, then b is a square if, and only if, b is an even power of ξ. In Definition 1.2 of Book C, Chapter 10, we introduced the term **quadratic residue of** p for a square of GF_p. Remember from Chapter 10, Subsection 1.1 that every non-zero square in GF_p has exactly two square roots, which differ just by sign.

Lemma 1.4

Suppose that p is an odd prime and that $p - 1 = 2^r s$, where s is odd and $r \geq 1$. Then, for every b such that $1 < b < p$, either $b^s \equiv 1 \,(\text{mod } p)$, or there exists a t, $0 \leq t \leq r-1$, such that $b^{2^t s} \equiv -1 \,(\text{mod } p)$.

Proof By Fermat's Little Theorem, for every integer b such that $1 < b < p$ we have $b^{p-1} \equiv 1 \,(\text{mod } p)$, or, equivalently, $b^{2^r s} \equiv 1 \,(\text{mod } p)$. We will now take a square root of this congruence. The square root of 1 mod p can only be one of $+1$ or -1, so that taking the square root gives

$b^{2^{r-1}s} \equiv \pm 1 \pmod{p}$. If the right-hand side of this congruence is -1, there is nothing more we can do. If, however, the right-hand side is $+1$ and $r \geq 2$, we may continue taking the square root again. Repeating this procedure we either reach some t, $0 \leq t \leq r-1$, such that $b^{2^t s} \equiv -1 \pmod{p}$, or we never reach such a t, in which case $b^s \equiv 1 \pmod{p}$. ■

In Subsection 1.4 we will need the contrapositive to this lemma, which we state as a separate corollary because it provides a useful sufficient condition for non-primality of a given integer.

Corollary 1.5

Suppose that k is an odd positive integer, $k \geq 3$, and that $k - 1 = 2^r s$, where s is odd and $r \geq 1$. If there exists an integer b, $1 < b < k$, such that $b^s \not\equiv 1 \pmod{k}$ and $b^{2^t s} \not\equiv -1 \pmod{k}$ for all t, $0 \leq t \leq r-1$, then k is not a prime number.

An integer b which satisfies the conditions of Corollary 1.5 is said to be a **witness of non-primality** for k.

Worked Exercise 1.6 *Witness of non-primality*

It is known that, for any positive integers ℓ and m, $2^\ell + 1$ divides $2^m + 1$ if, and only if, m is an odd multiple of ℓ. With the help of this fact, prove that $b = 2$ is a witness of non-primality for $k = 2^{2^n(2d+1)} + 1$ for any integers $n \geq 0$ and $d \geq 1$.

Solution

In the notation of Corollary 1.5 we have

$$k - 1 = 2^{2^n(2d+1)} \times 1,$$

so that $r = 2^n(2d+1)$ and $s = 1$. For $b = 2$ we have $b^s = b^1 = 2 \not\equiv 1 \mod k$. Let us now test the expression $b^{2^t s} = 2^{2^t}$ for $0 \leq t \leq r-1$. If $2^{2^t} \equiv -1 \mod k$ for some t such that $0 \leq t \leq r-1$, then $k = 2^r + 1$ would be a divisor of $2^{2^t} + 1$. By the fact stated in the formulation of this exercise, this would be possible only if 2^t was an odd multiple of $r = 2^n(2d+1)$, which is not the case as $d \geq 1$ implies that $r \geq 3$, so 2^t must be even. By Corollary 1.5, the integer $b = 2$ is a witness of non-primality of $k = 2^{2^n(2d+1)} + 1$.

The conclusion of Worked Exercise 1.6 does not apply to numbers of the form $F_n = 2^{2^n} + 1$, that is, without the odd factor in the exponent. Recall from Definition 2.7 of Book C, Chapter 9, that the integers F_n are known as the Fermat numbers, and for $n = 0, 1, 2, 3, 4$ they are actually prime numbers, called the Fermat primes.

Exercise 1.5

Find a witness of non-primality for $k = 289$.

We conclude with two results on finite fields. In Subsection 1.5 we will need a fast way of constructing a primitive element of a field GF_p for a prime p. We know from Corollary 3.5(b) of Chapter 18 that the number of primitive elements in the finite field of p elements, GF_p, is $\phi(p-1)$. Our current task is to identify a primitive element. This can be done with the help of the following criterion.

Lemma 1.7

Let p be a prime. A non-zero element $\xi \in GF_p$ is a primitive element of GF_p if, and only if, $\xi^{(p-1)/q} \not\equiv 1 \pmod{p}$ for all prime divisors q of $p-1$.

Proof If ξ is a primitive element, then the smallest positive power j such that $\xi^j \equiv 1 \pmod{p}$ is $p-1$. Since all the exponents $\frac{p-1}{q}$ for prime divisors q of $p-1$ are smaller than $p-1$, we have $\xi^{(p-1)/q} \not\equiv 1 \pmod{p}$ for any prime q dividing $p-1$.

Conversely, if ξ is not a primitive element of GF_p, then $\xi^d = 1$ for some positive integer d which is a proper divisor of $p-1$. Let q be a prime divisor of $\frac{p-1}{d}$. Then $\frac{p-1}{d} = bq$ for some positive integer b, which implies that $\frac{p-1}{q} = db$. But now $\xi^{(p-1)/q} = (\xi^d)^b = 1^b = 1$ in GF_p, and hence $\xi^{(p-1)/q} \equiv 1 \pmod{p}$ for some prime divisor q of $p-1$. ■

We illustrate this result in the next worked exercise.

Worked Exercise 1.8 *Finding a primitive element of GF_p*

Find a primitive element of GF_{193}.

Solution

For the prime $p = 193$ we have $p - 1 = 192 = 2^6 \times 3$, and so the prime divisors of $p-1$ are $q = 2, 3$. By Lemma 1.7, the exponents $\frac{p-1}{q}$ to be considered are 64 and 96.

Although the exponents appear to be high, we will show that the associated computations can be done quickly by the **squaring method**. The trick in this method is to write each exponent as a sum of powers of 2 (this can always be done: simply compute the binary expansion of the exponent). This is simple in our case, as $64 = 2^6$ and $96 = 2^6 + 2^5$. We then compute the powers with exponents of the form 2^j by repeated squaring and assemble the final result by multiplication. Here is how this procedure works in our example.

Since we have no clue as to which elements of GF_{193} might be primitive, we begin by experimenting with small numbers. The first candidate to try is 2. To check whether 2 is a primitive element of GF_{193} with the help of Lemma 1.7, we need to compute the residue classes of $2^{64} = 2^{2^6}$ and $2^{96} = 2^{2^6+2^5} = 2^{2^6} \times 2^{2^5}$ modulo 193. The computation of residue classes modulo 193 can be done even on most basic calculators by partial division. Following the outlined strategy of successive squaring, we obtain the following congruences modulo 193.

$$\begin{aligned}
2^{2^1} &= 2^2 = 4 \equiv 4 \\
2^{2^2} &= 4^2 = 16 \equiv 16 \\
2^{2^3} &= 16^2 = 256 \equiv 63 \\
2^{2^4} &= 63^2 = 3969 \equiv 109 \\
2^{2^5} &= 109^2 = 11\,881 \equiv 108 \\
2^{2^6} &= 108^2 = 11\,664 \equiv 84
\end{aligned}$$

We see that $2^{64} = 2^{2^6} \not\equiv 1 \pmod{193}$, which is promising. However, we find that
$2^{96} = 2^{2^6} \times 2^{2^5} \equiv 108 \times 84 = 9072 = 193 \times 47 + 1 \equiv 1 \pmod{193}$.
Thus, by Lemma 1.7, the element 2 is not primitive in GF_{193}.

The next obvious choice to try is the element 3. But now we find that $3^8 = 81^2 = 6561 \equiv -1 \pmod{193}$, and so $3^{64} \equiv 1 \pmod{193}$.
Lemma 1.7 now immediately implies that 3 is not a primitive element of GF_{193}, either.

The next smallest number to try is 4. But since we have found that 2 is not a primitive element of GF_{193}, neither is 4. (Why?) Thus, let us try our luck with 5. The method of squaring gives the following congruences modulo 193.

$$\begin{aligned}
5^{2^1} &= 5^2 = 25 \equiv 25 \\
5^{2^2} &= 25^2 = 625 \equiv 46 \\
5^{2^3} &= 46^2 = 2116 \equiv -7 \\
5^{2^4} &= (-7)^2 = 49 \equiv 49 \\
5^{2^5} &= 49^2 = 2401 \equiv 85 \\
5^{2^6} &= 85^2 = 7225 \equiv 84 \\
5^{2^6} \times 5^{2^5} &= 84 \times 85 = 7140 \equiv -1
\end{aligned}$$

We see that both 5^{64} and 5^{96} are not congruent to 1 modulo 193, and so by Lemma 1.7 we conclude that 5 is a primitive element of GF_{193}.

An algorithm to compute residue classes by the squaring method can be run on a rather basic calculator: all that is needed are built-in operations of addition, subtraction, multiplication, division, and storage in a memory cell. A formal version of such an algorithm will be given in Worked Exercise 1.12 of Subsection 1.3.

If you know some programming, you might like to try writing down an algorithm at this stage.

Exercise 1.6

Find a primitive element of GF_{257}.

Another preliminary result that we will need towards the end of this chapter, in Subsection 2.5, is Euler's Criterion (Book C, Chapter 10, Theorem 1.5). Euler's Criterion tells us how to recognise squares in the field GF_p, where p is an odd prime. We restate it here for reference, using the terminology and notation introduced in this chapter.

Lemma 1.9 *Euler's Criterion*

Let p be an odd prime and let b be a non-zero element of GF_p. Then b is a square in GF_p if, and only if, $b^{(p-1)/2} \equiv 1 \pmod{p}$, and b is a non-square in GF_p if, and only if, $b^{(p-1)/2} \equiv -1 \pmod{p}$.

Moreover, if $p \equiv -1 \pmod{4}$ and if b is a square in GF_p, then the two solutions of the equation $x^2 = b$ are $x = \pm b^{(p+1)/4}$.

We remark that there is no analogous formula for $p \equiv 1 \pmod{4}$. An efficient way of solving the equation $x^2 = b$ in such a case is the Tonelli–Shanks Algorithm, which is beyond the scope of this chapter.

Worked Exercise 1.10 *Squares and square roots in GF_p*

Determine whether 29 is a square in GF_{199}. If it is, find the solutions of the equation $x^2 = 29$ in GF_{199}.

Solution

For $p = 199$ we have $\frac{p-1}{2} = 99 = 2^6 + 2^5 + 2^1 + 2^0$, and we compute the residue class of $29^{99} \pmod{199}$ by the squaring method as in Example 1.8, but with all congruences modulo 199.

$$\begin{array}{rcrcrcr}
29^{2^1} & = & 29^2 & = & 841 & \equiv & 45 \\
29^{2^2} & = & 45^2 & = & 2025 & \equiv & 35 \\
29^{2^3} & = & 35^2 & = & 1225 & \equiv & 31 \\
29^{2^4} & = & 31^2 & = & 961 & \equiv & -34 \\
29^{2^5} & = & (-34)^2 & = & 1156 & \equiv & -38 \\
29^{2^6} & = & (-38)^2 & = & 1444 & \equiv & 51
\end{array}$$

This implies $29^{99} = 51 \times (-38) \times 45 \times 29 \equiv 1 \pmod{199}$, so 29 is indeed a square in GF_{199}. Since $199 \equiv -1 \pmod{4}$, we can actually determine the two solutions of $x^2 = 29$ in GF_{199} by applying the second part of Lemma 1.9 with the exponent $\frac{p+1}{4} = 50 = 2^5 + 2^4 + 2^1$ and using the above table to obtain

$$x = \pm 29^{2^5+2^4+2^1} \equiv (-38) \times (-34) \times 45 \equiv \pm 32.$$

Note that computations related to Euler's Criterion may be simplified further using Legendre symbols, as you saw in Book C, Chapter 10, Subsection 2.2.

Exercise 1.7

Determine whether -1, 3 and -5 are squares in GF_{193}. If they are, find their square roots.

We conclude this subsection with an important observation: when we use the squaring method to check whether a given element $k \in GF_p$ is a primitive element (or a square), the number of lines in the tabular form of the calculations is never larger than $\text{int}(\log_2 k)$. This means that even for enormously large values of k such as, say, $k \approx 2^{1000}$, we would obtain an answer in approximately a 1000-line table, that is, using a constant times 1000 arithmetic operations. Since such operations can be carried out extremely quickly on modern computers, checking for primitive elements or squares can be done in less than a blink of an eye even for numbers bigger than the estimated number of elementary particles in our universe! The same applies to multiplicative inverses of elements, as we noted in the short discussion after Exercise 1.3.

1.2 The RSA cryptosystem

Encryption and decryption procedures are usually described with the help of three characters: Alice (A), who needs to send a message to Bob (B) through an insecure channel where the data flow can be freely monitored by Eve (E), an eavesdropper.

Modern cryptosystems are designed for computer communication, and a message first needs to be converted into a form suitable for transfer through a digital channel. Most channels are binary, which essentially means that the signal flow through the channel can be imagined as a flow of 0s and 1s. Thus, messages need to be converted into binary numbers. However, to simplify matters and avoid doing binary arithmetic we will assume that messages are converted into decimal numbers.

There are numerous ways in which such a conversion can be done. One is to use some standard system, such as the ASCII code for representing capital and small letters of the alphabet, numerals, commas, etc. Another way could consist, for instance, in Alice and Bob agreeing to represent the letters A to Z by the numbers 1 to 26, and to represent a space by the number 27, say. So, for example, the message

'I NEED YOU'

would be represented by the number

09 271 405 050 427 251 521.

When the message to be transmitted is lengthy, it may be necessary to divide the resulting number into smaller pieces, but we will not go into such detail here. The point at issue is that the cryptosystems that we will look at in fact require numerical techniques.

The science of converting plaintext messages into streams of ciphers (typically, binary digits) is *coding theory*, which is a vast and exciting area of mathematics. It differs from cryptography in that the main concern of coding theory is the development of methods for detection and correction of errors in the data flow, rather than the protection of data from eavesdropping.

With the algebraic preliminaries of Subsection 1.1, we are ready to describe the RSA public-key cryptosystem.

Communication setup

In order to start the procedure for secure communication, Bob needs to set up a pair of parameters. He chooses two distinct odd primes p and q and calculates their product $n = pq$. Since he knows the prime factorisation of n, he determines the value of Euler's ϕ-function $\phi(n) = (p-1)(q-1)$. Bob then chooses an integer e that is relatively prime to $\phi(n)$ and such that $1 < e < \phi(n)$. He then releases the pair (n, e) through the communication channel so that everybody, including Alice and Eve, can get hold of this information.

We emphasise that Bob does not release the two primes p, q. In fact, he can discard them, since for communication he will only need the public key (n, e) and the value of $\phi(n)$. The final preparatory move for Bob is to determine the multiplicative inverse to e modulo $\phi(n)$, that is, the unique d such that $1 < d < \phi(n)$ and $de \equiv 1 \pmod{\phi(n)}$. This can be done with the help of the Fast Euclidean Algorithm as in Worked Exercise 1.2. Unlike for the pair (n, e), Bob does not release the value of d.

We sum up the list of required parameters as a definition.

Definition 1.11 *RSA triple, public key, private key*

Let $n = pq$ be a product of two distinct primes p, q and let e be a positive integer such that $1 < e < \phi(n)$ and e is relatively prime to $\phi(n)$. Let d be the unique positive integer such that $1 < d < \phi(n)$ and $de \equiv 1 \pmod{\phi(n)}$. Then:

(a) the triple (p, q, e) is called an **RSA triple**

(b) the pair (n, e) is the **public key**

(c) the integer d is the **private key**.

The reason why the pair (n, e) is called the public key and the integer d is called the private key is that Bob releases the pair (n, e) to the public, but keeps d for himself.

We are now ready to describe the encryption and decryption procedures.

Encryption

The encryption procedure depends only on the public key (n, e). Alice begins by converting her message into a number m such that $1 < m < n - 1$; we have mentioned ways to do this earlier. As the next step, Alice uses the public key (n, e) to compute the number

$$c \equiv m^e \pmod{n}.$$

Finally, she sends c to Bob through an appropriate channel. Note that we have deliberately chosen the notation so that m stands for *m*essage and c for *c*iphertext.

Decryption

From the point of view of abstract algebra, the decryption procedure is astonishingly simple. Bob receives c and, knowing n and d, calculates the value $c^d \pmod{n}$. What does he obtain as a result? The 'insider information' that $c = m^e \pmod{n}$ combined with Lemma 1.3 gives

$$c^d \equiv (m^e)^d = m^{de} \equiv m \pmod{n}$$

and hence $c^d \pmod{n}$ is equal to m. In other words, by raising c to the power equal to his private key, Bob has decrypted Alice's message!

Eavesdropping?

Eve, the eavesdropper, can intercept n, e and c by monitoring the communication through the channel. Assuming that she knows how RSA works, is she in a position to decipher the message m with only the knowledge of n, e and c? The answer is in the affirmative if she can factor n: if she can find p and q, she can determine $\phi(n)$ and hence the inverse d of e modulo $\phi(n)$, and then she can decrypt the ciphertext exactly as Bob can. However, in Subsection 1.4 you will see that, in general, factorising n into his prime factors is not feasible, provided the primes p and q chosen by Bob are sufficiently large. In the same subsection we will also discuss other hypothetical ways to 'break' RSA.

1.3 Examples of RSA cryptosystems

We illustrate RSA encryption and decryption in detail in the next example.

Example 1.12 *RSA encryption and decryption*

Suppose that Alice needs to send Bob the message 619, which is the three-digit security number on her Visa credit card, for him to complete an online purchase. To avoid lengthy calculations in this model example, we assume that Bob chooses two small primes, say $p = 61$ and $q = 97$. The product is then $n = pq = 5917$ and the corresponding value of Euler's ϕ-function is

$$\phi(n) = (p - 1)(q - 1) = 5760.$$

Bob now needs to choose an exponent e that is relatively prime to 5760 and is such that $1 < e < 5760$, and then determine the multiplicative inverse of e modulo 5760. For relatively small numbers, such as the ones in this example, Bob can carry out both tasks simultaneously: to choose the exponent e and have its multiplicative inverse d modulo 5760 at the same time, Bob can successively try to factor the integers of the form $5760t + 1$ for $t = 1, 2, \ldots$. From the factorisations he obtains in this way, he chooses any two e and d such that $de = 5760t + 1$. He finds that $t = 8$ gives

$$5760 \times 8 + 1 = 46\,081 = 7 \times 29 \times 227 = 203 \times 227,$$

which is a factorisation he likes. So he chooses $e = 203$ and releases the public key $(n, e) = (5917, 203)$, keeping the private key $d = 227$ for himself.

Alice's message is her three-digit security number, $m = 619$. Using the public key, she now needs to determine the unique positive integer c such that $c \equiv m^e \pmod{n}$, that is, $c \equiv 619^{203} \pmod{5917}$. This calculation might look scary at a first glance, but we will show that it can be performed quickly even using a very modest calculator.

The key is to use the squaring method: Alice writes the exponent 203 as a sum of powers of 2, that is,

$$203 = 128 + 64 + 8 + 2 + 1 = 2^7 + 2^6 + 2^3 + 2^1 + 2^0.$$

Then, letting $m_0 = m$, she successively determines

$$\begin{aligned}
m_1 &= m_0^2 \equiv m^{2^1} \pmod{n} \\
m_2 &= m_1^2 \equiv m^{2^2} \pmod{n} \\
m_3 &= m_2^2 \equiv m^{2^3} \pmod{n} \\
&\vdots \qquad \vdots \qquad\quad \vdots \\
m_7 &= m_6^2 \equiv m^{2^7} \pmod{n}.
\end{aligned}$$

Finally, she computes

$$c \equiv m^{203} = m^{2^7+2^6+2^3+2^1+2^0} \equiv m_7 m_6 m_3 m_1 m_0 \pmod{n}.$$

Alice can do this quickly with the help of a basic calculator. She stores $n = 5917$ in the memory and keeps to the following simple algorithm.

(0) Set $i = 1$; the value of i is your counter (which can be recorded, say, on a piece of paper).

(1) Input m_{i-1} and compute m_{i-1}^2 (by, say, multiplying m_{i-1} by itself), leaving the result on the display.

(2) Divide m_{i-1}^2 by n (to enter n use the 'Read Memory' key).

(3) From the result on the display, subtract its integer part; this leaves on the display a number greater than 0 and smaller than 1.

(4) Multiply the displayed number by n; if necessary, round the result to the nearest integer.

(5) The number on the display is now m_i; record this result.

(6) If $i = 7$, then stop; otherwise increase i by 1 and go to step (1).

Note that steps (3) and (4) simply determine the remainder after partial division by n. The final step, that is, determination of $c \pmod n$, can again be performed using steps (3) and (4) appropriately.

Alice's encryption

Alice runs the algorithm we have just described with the help of her calculator and records the following partial results modulo 5917:

$$\begin{aligned}
&m_0 = 619,\\
&m_0^2 = 383\,161, && m_1 \equiv m_0^2 \equiv m^{2^1} \equiv 4473\\
&m_1^2 = 20\,007\,729, && m_2 \equiv m_1^2 \equiv m^{2^2} \equiv 2352\\
&m_2^2 = 5\,531\,904, && m_3 \equiv m_2^2 \equiv m^{2^3} \equiv 5426\\
&m_3^2 = 29\,441\,476, && m_4 \equiv m_3^2 \equiv m^{2^4} \equiv 4401\\
&m_4^2 = 19\,368\,801, && m_5 \equiv m_4^2 \equiv m^{2^5} \equiv 2460\\
&m_5^2 = 6\,051\,600, && m_6 \equiv m_5^2 \equiv m^{2^6} \equiv 4426\\
&m_6^2 = 19\,589\,476, && m_7 \equiv m_6^2 \equiv m^{2^7} \equiv 4206.
\end{aligned}$$

Having computed all the ingredients, Alice determines the product $m^{203} \equiv m_7 m_6 m_3 m_1 m_0 \pmod{5917}$ as follows:

$$\begin{aligned}
&m_7 m_6 = 18\,615\,756 \equiv 874 \pmod{5917}\\
&m_7 m_6 m_3 = 874 m_3 = 4\,742\,324 \equiv 2807 \pmod{5917}\\
&m_7 m_6 m_3 m_1 = 2807 m_1 = 12\,555\,711 \equiv 5754 \pmod{5917}.
\end{aligned}$$

The final result is

$$c = m_7 m_6 m_3 m_1 m_0 \equiv 5754 m_0 = 3\,561\,726 \equiv 5609 \pmod{5917}.$$

It follows that the ciphertext that Alice transmits to Bob is $c = 5609$.

Bob's decryption

Bob too uses the squaring method to write his private key $d = 227$ as a sum of powers of 2:

$$227 = 128 + 64 + 32 + 2 + 1 = 2^7 + 2^6 + 2^5 + 2^1 + 2^0.$$

Letting $c_0 = c$, he successively computes $c_1 \equiv c^{2^1} \pmod n$, $c_2 \equiv c_1^2 = c^{2^2} \pmod n$, $c_3 \equiv c_2^2 = c^{2^3} \pmod n$, and so on, up to $c_7 \equiv c_6^2 = c^{2^7} \pmod n$, and using these he finally determines

$$c^{227} = c^{2^7+2^6+2^5+2^1+2^0} \equiv c_7 c_6 c_5 c_1 c_0 \pmod n.$$

Through these individual steps, Bob obtains the following results modulo 5917:

$$\begin{aligned}
&c_0 = 5609,\\
&c_0^2 = 31\,460\,881, && c_1 \equiv c_0^2 \equiv c^{2^1} \equiv 192\\
&c_1^2 = 36\,864, && c_2 \equiv c_1^2 \equiv c^{2^2} \equiv 1362\\
&c_2^2 = 1\,855\,044, && c_3 \equiv c_2^2 \equiv c^{2^3} \equiv 3023\\
&c_3^2 = 9\,138\,529, && c_4 \equiv c_3^2 \equiv c^{2^4} \equiv 2681\\
&c_4^2 = 7\,187\,761, && c_5 \equiv c_4^2 \equiv c^{2^5} \equiv 4523\\
&c_5^2 = 20\,457\,529, && c_6 \equiv c_5^2 \equiv c^{2^6} \equiv 2460\\
&c_6^2 = 6\,051\,600, && c_7 \equiv c_6^2 \equiv c^{2^7} \equiv 4426.
\end{aligned}$$

He can now compute $c^{227} \equiv c_7c_6c_5c_1c_0 \pmod{5917}$:

$$c_7c_6 = 10\,887\,960 \equiv 680 \pmod{5917}$$
$$c_7c_6c_5 \equiv 680c_5 = 3\,075\,640 \equiv 4717 \pmod{5917}$$
$$c_7c_6c_5c_1 \equiv 4717c_1 = 905\,664 \equiv 363 \pmod{5917}.$$

The final result is

$$c^{227} \equiv c_7c_6c_5c_1c_0 \equiv 363c_0 = 2\,036\,067 \equiv 619 \pmod{5917},$$

so $m = 619$, which is indeed Alice's three-digit security number!

It is important to note that both Alice's encryption and Bob's decryption can be carried out quickly. Indeed, in general, if m is Alice's message and $1 < m < n$, then one needs at most $\text{int}(\log_2 m)$ squarings modulo n, and then at most another $\text{int}(\log_2 m)$ multiplications modulo n. Since $m < n$, one needs to perform no more than $2\ \text{int}(\log_2 n)$ multiplications modulo n to encrypt an arbitrary message! So RSA encryption and decryption can be carried out rapidly even for extremely large numbers – in less than a blink of an eye on a rather low-performance notebook.

Exercise 1.8 *RSA encryption and decryption*

Alice wants to transmit the message $m = 1111$ to Bob using the RSA cryptosystem with public key $(5963, 203)$.

(a) Determine Alice's ciphertext c.

(b) Given that Bob's private key $d = 515$, verify that his decryption produces Alice's message.

1.4 How secure are RSA cryptosystems?

Let us now examine the security of RSA cryptosystems in more detail. We mentioned the threat posed by a potential eavesdropper, Eve, at the end of Subsection 1.2. What are Eve's chances of deciphering the message m by eavesdropping? By monitoring communication through the channel, Eve can get hold of the public key (n, e) and of the ciphertext, that is, the integer c. We may safely assume that Eve has passed M303 with a distinction, and so she is fully familiar with RSA encryption. This means that Eve knows that Alice's message, an integer m such that $1 < m < n$, has been raised to the power e. Eve also knows that c, the ciphertext sent through the channel, is the remainder of the partial division of m^e by n, where n is known. The question now is whether this knowledge is enough for Eve to determine m.

Eve could certainly decrypt Alice's message if she knew Bob's private key d, as then she would simply follow the decryption procedure. So our question is really whether Eve can determine d from n and e. Since Eve knows that d is the multiplicative inverse of e modulo $\phi(n)$, it would be sufficient for her to determine $\phi(n)$ and then use the Euclidean Algorithm to calculate d as we did in Worked Exercise 1.2.

At this stage you might think that determining $\phi(n)$ should be easy. Since Eve knows the workings of RSA, she also knows that n is the product of two distinct primes p and q. Thus, it is sufficient for Eve to factor n into p and q, and hence recover $\phi(n) = (p-1)(q-1)$.

And now comes the important fine point. Suppose Bob chooses p and q in such a way that their product, n, is enormously large – say, requiring about 1000 bits (binary digits) to be represented in the binary system. To translate this into the decimal system, the approximation $2^{10} \approx 10^3$ tells us that a 1000-bit number would require about 300 decimal digits to be written in decimal notation. Let us assess the feasibility of factoring such a large number.

Prime factorisation: a naive approach

If n is not a prime, it must contain a prime factor not exceeding $\sqrt{n}$. By way of an example, assume that n is only a 300-bit number (that is, with about 90 decimal digits) and let us look for a 150-bit prime factor of n.

In total, there are $t = 2^{150} - 2^{149} = 2^{149}$ 150-bit numbers. As a consequence of the Prime Number Theorem (see Book A, Chapter 2, Subsection 4.3), the number of 150-bit primes is approximately $\frac{t}{\log t}$. We now make a number of rather crude estimates to simplify the numbers we will be working with. For $t = 2^{149}$ we have

$$\frac{t}{\log t} > \frac{t}{\log_2 t} = \frac{2^{149}}{149} > 2^{140} = (2^{10})^{14} > (10^3)^{14} = 10^{42}.$$

So there would be approximately 10^{42} 150-bit primes not exceeding $\sqrt{n}$.

Let us, rather unrealistically, assume that we were able to generate all such primes, so that we could run a trivial algorithm to factorise n by successively dividing n by each of these primes.

If we used a science-fiction super-computer capable of carrying out a single division in one picosecond, that is, in 10^{-12} seconds, in one second we would be able to divide by 10^{12} (a thousand billion) 150-bit primes. In the worst case, however, we would have to try to divide by all the (at least) 10^{42} such primes. This would take $\frac{10^{42}}{10^{12}} = 10^{30}$ seconds. Realising that one year has about 31.5 million (that is, approximately 3.15×10^7) seconds, you see that even under our optimistic assumptions the computation could take longer than 10^{22} years in the worst case! Even a million such computers would not help much – the computing time would be reduced to (longer than) $\frac{10^{22}}{10^6} = 10^{16}$ years!

Prime factorisation: the general number sieve algorithm

The prime factorisation algorithm that we have just described is rather naive, as to factorise n we simply test for all possible prime factors not exceeding $\sqrt{n}$. Arguably, better factorisation algorithms should be available. Currently, the best algorithm available is the **general number sieve algorithm**. This is a very sophisticated procedure well beyond the scope of this module and here we can only give a general idea of how the algorithm operates.

The idea behind the general number sieve algorithm is as follows. To find a prime factor of a given positive integer n, the algorithm uses the theory of algebraic extensions of the ring of integers to produce, in a highly non-trivial way, a pair of positive integers $x > y$ such that n divides $x^2 - y^2$ and $n \neq x + y, x - y$. If p is a prime factor of n, then p is a divisor of $x - y$ or $x + y$. The Fast Euclidean Algorithm determines $\mathrm{hcf}(n, x - y)$ and $\mathrm{hcf}(n, x + y)$; one of these must contain p as a factor.

If n is a number of at least 100 decimal digits, it has been estimated that, in the worst case, factorising n using the general number sieve algorithm requires about $\exp[c(\log n)^{1/3}(\log(\log n))^{2/3}]$ 'operations', where c is a constant. We have put the word 'operations' in quotation marks because the value of the constant c depends on what one understands by an 'operation'. Let us assume that an 'operation' is either addition, subtraction, multiplication or division. For simplicity we will rather unrealistically assume that each of these operations takes the same amount of time. The theory underlying the algorithm then shows that the constant c may be replaced by 2 for, say, 1000-digit numbers.

Now suppose that the magnitude of n is approximately 2^{1000}, that is, the binary representation of n requires about 1000 digits (and hence the decimal representation requires about 300 digits). Since $\log_2 n \approx 1000$ and $\log 2 \approx 0.7$, a quick calculation shows that

$$\log n \approx 1000 \log 2 \approx 700 \quad \text{and} \quad \log(\log n) \approx 6.55.$$

For $c = 2$ this approximation gives

$$2(\log n)^{1/3}(\log(\log n))^{2/3} \approx 70.$$

By the above estimate we may assume, for the sake of an example, that the general number sieve algorithm needs no more than $e^{70} \approx 2^{100} \approx 10^{30}$ operations to factor n. If we were to run the algorithm on $3000 = 3 \times 10^3$ machines, and if a single operation took 10^{-9} seconds on each of these machines, in the worst case factoring n would take about $10^{30}/(3 \times 10^3 \times 10^9 \times 3.15 \times 10^7) \approx 10^9$ years. This is much shorter than the time required by the naive algorithm, and for a much larger number, but still very long!

The above estimates were made under numerous simplifications and still refer to the worst case, so that the actual running time for a concrete n might be considerably shorter. The greatest success of the general number sieve algorithm, implemented with a number of further mathematical subtleties, has been the factorisation of a 232 decimal digit number on hundreds of machines over a span of more than 2 years, finished in 2009.

The current recommendation for safe RSA communication is to use numbers that are approximately 1000 bits long, and approximately 2000 bits long if super extra security is required.

Generating large primes: The Rabin–Miller test

The next question we need to address is how to generate large prime numbers so as to find suitable parameters for RSA. Our previous discussion suggests that simply taking a random large number (say, 200 digits long) and trying to factor it is infeasible, so we cannot hope to find large primes in this way. Luckily, there appears to be a huge difference between testing a number for primality and factorising it into its prime divisors.

To explain the idea of primality testing without factorisation, let us assume that we want to test a (large) odd positive integer $k \geq 3$. Since k is odd, there are positive integers r and s such that s is odd and $k - 1 = 2^r s$. Now take an integer b such that $1 < b < k$ and consider the following statement $S(b)$:

$$S(b): \; b^s \not\equiv 1 \,(\mathrm{mod}\ p) \text{ and } b^{2^t s} \not\equiv -1 \,(\mathrm{mod}\ p) \text{ for all } t \text{ such that } 0 \leq t \leq r-1.$$

Recall that, in Subsection 1.1, a positive integer b for which $S(b)$ is a true statement was called a **witness of non-primality** for k. The next lemma explains this choice of terminology.

Lemma 1.13 *Witness of non-primality*

Let k be an odd positive integer, $k \geq 3$, and let $k - 1 = 2^r s$ where r and s are positive integers and s is odd. If the statement $S(b)$ is true for some b such that $1 < b < k$, then k is not a prime.

Proof This is just a re-statement of Corollary 1.5 of Subsection 1.1. ■

Now, what happens if the statement $S(b)$ is false for, say, j distinct random integers b such that $1 < b < k$? We cannot be sure that k is a prime in such a case. However, it can be shown that in this case the probability that k is *not* a prime is less than 4^{-j}. This is the basis of the **Rabin–Miller test**; integers k that have passed the test, that is, such that $S(b)$ is false for j values of b, are called **strong probable primes to base** b.

The Rabin–Miller test

To test a given positive integer k for primality, we choose a positive integer j. We then randomly generate j distinct integers b such that $1 < b < k$. If $S(b)$ is false for all the j values of b, we accept k as a strong probable prime, and then the probability that k is a prime is at least $1 - 4^{-j}$.

Thus, for example, if k is a 150-bit number k and $S(b)$ is false for $j = 40$ randomly chosen values of b strictly between 1 and k, then the probability of k failing to be a prime is less than $2^{-80} < 10^{-24}$. For practical purposes we may therefore treat the strong positive prime k as if it was a prime number.

The estimates we have presented are rather crude, yet they are enough to show the power of the mathematical theory behind the Rabin–Miller test. In practice, testing whether a large, random odd, say 150-bit number k is prime requires generating just about 20 numbers b strictly between 1 and k. If $S(b)$ is false for all the generated bs, then we declare k to be a prime, and we will be right with very high probability. If $S(b)$ happens to be true for just one of these bs, then we need to generate another k and repeat the Rabin–Miller test.

The question remains of how quickly we can generate a number that would pass the Rabin–Miller test. We illustrate the answer by way of an example, again. Let us go back to our 150-bit numbers and recall that among the $t = 2^{149}$ such numbers there are approximately $\frac{t}{\log t}$ primes. Another important result on the distribution of primes says that the average gap between two consecutive primes has length approximately equal to $\log t$. Now observe that

$$\log t = \log(2^{149}) = 149 \log 2 \approx 100.$$

So if a random, odd 150-bit number k is not a prime, one of the numbers $k+2, k+4, \ldots, k+100$ will be a prime with very high probability. It follows that, on the average, the Rabin–Miller test will return a 150-bit number that can be considered a prime after at most 50 trials! In practice, about half of this theoretical average number of trials is usually sufficient.

The Rabin–Miller test can be performed rapidly, since powers modulo k can be computed rapidly, as you saw in the solution to Example 1.12.

We would like to emphasise the difference between primality testing and factorisation again, using a slightly different point of view. Let k be an enormously large odd number such that $k - 1 = 2s$, where s is odd. Assume that k fails the Rabin–Miller test. In this particular case, failing the test means that a number b strictly between 1 and k has been generated such that $b^s \equiv \pm 1 \pmod{k}$. Then, by Corollary 1.5, we know that k is not a prime. Nevertheless, we saw that finding the actual factorisation of such a k is infeasible!

Other ways of attacking the RSA cryptosystem?

Recall that we actually want to find out whether Eve can determine $\phi(n)$ from n without knowing the factorisation pq. Could there be some indirect way of revealing the value of $\phi(n)$? If there were one, then, from $n = pq$ and $\phi(n) = pq - (p+q) + 1$ we would obtain two equations in two unknowns p and q, namely

$$p + q = n + 1 - \phi(n) \quad \text{and}$$
$$pq = n,$$

from which we would be able to determine p and q. But since we saw that there is no 'easy' way to determine the two primes, there cannot be an easy way to determine $\phi(n)$.

A deeper analysis, beyond the scope of this module, actually shows that if there was any 'easy' indirect way of deciphering a general ciphertext c just on the basis of the public key (n, e), then there would be an 'easy' way to determine the two prime factors of n. Since the latter is infeasible for extremely large n, the practical conclusion is that RSA is 'reasonably safe in general'. The addendum 'in general' means that one cannot completely exclude instances when RSA is unsafe, but these occur with negligible probability.

1.5 The Diffie–Hellman cryptosystem

In this subsection we will look at another cryptosystem based on modular arithmetic. Its security, however, is not be based on the infeasibility of prime factorisation, but on the so-called *discrete logarithm problem*, which we will introduce in the course of our explanation.

Communication setup

As before, our two characters Alice and Bob want to communicate securely through an insecure channel. They agree on using a prime p and all the necessary calculations for communication will be done in the field GF_p, or, equivalently, modulo p. For a fast generation of large integers that are prime with high probability, they use the Rabin–Miller test from Subsection 1.4. They further agree a fixed primitive element $\xi \in GF_p$. We have seen that a primitive element can be generated quickly with the help of Lemma 1.7 and the process was illustrated in the solution to Worked Exercise 1.8. The pair (p, ξ) is the public key that Alice and Bob release.

As the next step, Alice chooses a positive integer a such that $1 < a < p - 1$, and Bob chooses a positive integer b such that $1 < b < p - 1$. The integer a is Alice's private key and b is Bob's private key.

The communication is initiated as follows. Alice calculates $\alpha = \xi^a$ in GF_p, or, equivalently, $\alpha \equiv \xi^a \pmod{p}$ with $1 \leq \alpha \leq p - 1$, and sends the number α over the channel to Bob. Symmetrically, Bob calculates $\beta = \xi^b \bmod p$ and sends β to Alice. The numbers α and β are sent through an insecure channel, and so can become public knowledge.

Still as part of the setup, Alice computes β^a in GF_p using her private key a and Bob computes α^b with the help of his private key b. Observe that they must obtain the same result, since

$$\beta^a = (\xi^b)^a = (\xi^a)^b = \alpha^b.$$

We will denote the common value $\beta^a = \alpha^b = \xi^{ab}$ by σ. The value of σ will not be released during the communication; it is a **shared secret** between Alice and Bob.

Now, both Alice and Bob can determine σ^{-1}, the multiplicative inverse of σ in GF_p, and they can do it in two ways. One way is to run the Fast Euclidean Algorithm for the pair of relatively prime numbers σ and p, as in Worked Exercise 1.2. But there is a second way of doing this: Bob

knows α and, using his private key b, he can evaluate α^{p-1-b}. With his insight into the communication scheme, and using $\xi^{p-1} = 1$, he obtains

$$\alpha^{p-1-b} = (\xi^a)^{p-1-b} = (\xi^{p-1})^a \xi^{-ab} = 1 \times \sigma^{-1} = \sigma^{-1}.$$

Similarly, Alice can determine σ^{-1} by simply computing β^{p-1-a}.

Encryption and decryption

The information exchange can now go both ways as follows. Suppose that Alice wants to send Bob a message coded as $m \in GF_p$. She computes the product $c = m\sigma$ in GF_p, and transmits the ciphertext c through the channel to Bob. To decrypt, Bob just needs to multiply the ciphertext c by σ^{-1} to obtain the original message m. Bob uses the same encryption technique if he wants to send a message to Alice.

Example 1.14 *Diffie–Hellman encryption and decryption*

Suppose again that Alice wants to send Bob her three-digit credit card security number $m = 196$. For the sake of this demonstration example, they agree to use the prime $p = 257$.

The fact that $257 = 2^8 + 1$ enables Alice and Bob to quickly determine a primitive element of GF_{257}: they see right away that

$$2^8 \equiv -1 \pmod{257},$$

so that 2 cannot be a primitive element. How about 3? As $3^4 = 81$, Alice and Bob quickly check that, in GF_{257}, $3^8 = 136$ and $3^{16} = -8 = -2^3$. Further, in GF_{257} they also have $3^{32} = 2^6$, $3^{64} = 2^{12} = -2^4$, and finally $3^{128} = 2^8 = -1$. This means that 3 is a primitive element, since $3^{256} = 1$, and the fact that $3^{128} = -1$ proves that the multiplicative order of 3 in GF_{257} is indeed 256.

Alice and Bob can now choose as their ξ any power 3^j where j is relatively prime to 256, and they choose 3^{29}. To evaluate this power in GF_{257}, which is equivalent to evaluating $3^{29} \pmod{257}$, they use our well-known trick of writing the exponent as a sum of powers of 2:

$$3^{29} = 3^{16} \times 3^8 \times 3^4 \times 3 \equiv -8 \times 136 \times 81 \times 3 \equiv 69 \pmod{257},$$

and so they set $\xi = 69$.

Again, just to simplify calculations, Alice and Bob choose $a = 13$ and $b = 17$ as their private keys respectively. Alice computes the element $\alpha = \xi^a = 69^{13} = 51$ in GF_{257} and sends α to Bob, while Bob computes $\beta = \xi^b = 69^{17} = 163$ and sends this value to Alice. Then Alice determines

$$\sigma = \beta^a = 163^{13} = 163^8 \times 163^4 \times 163 = 151,$$

and Bob computes

$$\alpha^b = 51^{17} = 51^{16} \times 51 = 151,$$

all in GF_{257}. From our discussion of the communication setup, we know that they must obtain the same value, namely, $\sigma = 151$.

Again from our previous discussion, we know how both Alice and Bob can evaluate σ^{-1}. One way would be to determine the multiplicative inverse of 151 modulo 257 using the Fast Euclidean Algorithm; we did this in Worked Exercise 1.2. To use the second possibility outlined earlier, say from Bob's perspective, in GF_{257} he can compute

$$\sigma^{-1} = \alpha^{p-1-b} = 51^{239} = 51^{128+64+32+8+4+2+1} = 80,$$

which agrees with the solution of Worked Exercise 1.2.

Recall that Alice's message was $m = 196$. In GF_{257}, she computes

$$c = m \times \sigma = 196 \times 151 = 41$$

and sends this number to Bob, who decrypts the message c by simply working out $c \times \sigma^{-1} = 41 \times 80 = 196$ in GF_{257}.

Exercise 1.9

Alice and Bob want to exchange some information using the Diffie–Hellman cryptosystem with $p = 193$, $\xi = 5$. Alice chooses $a = 12$ as her private key and Bob chooses $b = 17$ as his. If Alice's message is $m = 123$, determine the ciphertext c and verify that Bob's decryption of the ciphertext gives back Alice's message.

Security

In order to ensure security in a Diffie–Hellman exchange, one would have to choose an enormously large prime number p to begin with. An analysis of the encryption and decryption algorithms then shows that if there was an 'easy' way to decrypt messages, then there would be an 'easy' way to determine Alice's and Bob's secret exponents a and b. If this was the case, there would be an 'easy' way to determine the exponent a from the publicly known values of ξ and $\alpha = \xi^a$. If α and ξ were positive real numbers, then the value of a would simply be equal to $\log_\xi \alpha$. However, it is far from clear how to compute a when α and ξ are elements of the finite field GF_p. It turns out that we may still think of a as a generalisation of a logarithm, for which we give the following definition.

Definition 1.15 *Discrete logarithm in finite fields*

Let $\alpha \neq 0$ and $\beta \neq 0, 1$ be elements of a finite field GF_p. If there exists an integer a such that $0 \leq a < p - 1$ and $\beta^a = \alpha$, then a is called the **discrete logarithm of α to the base β**. In such a case we write $a = \log_\beta \alpha$.

Observe that if $\beta = \xi$, a primitive element of GF_p, then the discrete logarithm always exists and is uniquely determined. So determining the exponent a in the previous paragraph is equivalent to determining the discrete logarithm $a = \log_\xi \alpha$.

However, it turns out that computing discrete logarithms in the field GF_p appears infeasible for very large primes p (at least several hundreds of decimal digits long) in real time. The lack of fast algorithms for computing discrete logarithms thus provides assurance that, in general, Diffie–Hellman encryption can be considered safe if the prime p and the primitive element ξ are chosen properly (again, going into more detail is well beyond our scope here).

The Diffie–Hellman system is rarely used in practice, mostly due to commercial reasons. The dominant public-key cryptosystems are based on RSA and, increasingly, on elliptic curves, which you will meet in the next section. We have included the Diffie–Hellman system in this chapter to present a cryptosystem based on the apparent infeasibility of the discrete logarithm problem. A generalisation of this problem is essential for the security of cryptosystems based on elliptic curves, which we are about to describe.

2 Cryptosystems based on elliptic curves

Under certain mild restrictions, an elliptic curve over a field F with constants $a, b \in F$ can be identified with the graph of the implicit function given by the equation $y^2 = x^3 + ax + b$, that is, with the set of all ordered pairs $(x, y) \in F \times F$ that satisfy the equation. If the underlying field F is the field of rational numbers, the corresponding elliptic curves play a decisive role in the proof of the famous Fermat's Last Theorem. Surprisingly, elliptic curves over a finite field have found non-trivial applications in public-key cryptography; such applications were suggested independently by Neal Koblitz and Victor S. Miller in 1985.

In this section we present a light version of the mathematical background needed to understand elliptic curves over various fields. Subsection 2.1 contains basic facts about cubic polynomials. Elliptic curves are formally defined in Subsection 2.2, with a number of examples. The striking feature of elliptic curves is that they give rise to an abelian group in a natural way, which we introduce in Subsection 2.3 and illustrate through some examples in Subsection 2.4. Finally, in Subsection 2.5 we introduce two cryptosystems based on elliptic curves over finite fields, the ElGamal and the Menezes–Vanstone systems. We also include a discussion on the security of these systems, which is based on an analogue of the discrete logarithm problem for elliptic curves.

2.1 First things first: cubic polynomials

Let F be a field. At this point we make no assumptions about F: it can be finite or infinite, although later we will focus on finite fields. As we shall

soon see, elliptic curves are defined by means of cubic polynomials over a field. Therefore we start by looking at such polynomials in some detail.

A general cubic polynomial over F with leading term equal to 1 has the form

$$z^3 + Az^2 + Bz + C, \quad \text{where} \quad A, B, C \in F. \tag{1}$$

If the characteristic of the field is not equal to 3, then the element $3 = 1 + 1 + 1 \in F$ is not equal to zero and hence has a multiplicative inverse in F, which we denote by $\frac{1}{3}$ as usual. In this case, we may make the substitution $z = x - \frac{1}{3}A$ in (1), which gives

$$\left(x - \frac{1}{3}A\right)^3 + A\left(x - \frac{1}{3}A\right)^2 + B\left(x - \frac{1}{3}A\right) + C. \tag{2}$$

Evaluating the powers and simplifying, turn the polynomial (2) into

$$x^3 + ax + b, \quad \text{where} \quad a = -\frac{1}{3}A^2 + B, \quad b = \frac{2}{27}A^3 - \frac{1}{3}AB + C. \tag{3}$$

Expression (3) tells us that if the characteristic of the field is not 3, we may simplify a cubic polynomial with leading term 1 by removing the term containing the square of the indeterminate. Therefore from now on we will only consider cubic polynomials over a field F of the form

$$f(x) = x^3 + ax + b, \quad a, b \in F. \tag{4}$$

In doing so, we will take into the account the loss of generality when the characteristic of the field is equal to 3 – no loss of generality occurs for fields of characteristic distinct from 3. In addition, we will restrict the discussion to the case when $f(x)$ has no multiple roots. We delay an explanation of the reason for this restriction until after Proposition 2.14 in Subsection 2.3.

In the terminology introduced at the end of Book B, Chapter 7, Subsection 4.2, cubic equations (that is, polynomial equations of degree 3) can be solved by radicals. A formula for the solution was discovered by the Italian mathematician Gerolamo Cardano in medieval times, and it is far more complex than the formula for solving quadratic equations. However, a sufficient condition for a cubic polynomial of the form $x^3 + ax + b$ to have no multiple root can be obtained surprisingly easily, and without invoking Cardano's formula.

Lemma 2.1

Let $f(x) = x^3 + ax + b$ be a polynomial over an arbitrary field F. If $4a^3 + 27b^2 \neq 0$, then $f(x)$ has no multiple roots.

You are asked to prove Lemma 2.1 in the next exercise. Observe that we do not assume that the characteristic of the field is different from 2 and 3, so even in such fields $4a^3 + 27b^2 \neq 0$ is a sufficient condition for $f(x) = x^3 + ax + b$ to have no multiple roots, but we will not need this fact.

Exercise 2.1 *Proof of Lemma 2.1*

Prove Lemma 2.1.

Hint: try proving the contrapositive.

In the next section we will need more information about the behaviour of the graphs of cubic polynomials over the field $\mathbb{R}$ of real numbers. To derive this information, we will recall how to sketch the graph of $f(x)$ in the real plane with the help of the first and the second derivative. You are likely to have met this method to graph real functions in any calculus courses in your previous mathematical studies.

Thus, let $f(x) = x^3 + ax + b$ be such that the coefficients a, b and the values of f are real numbers. The derivative $f'(x) = 3x^2 + a$ has no real roots if $a > 0$, and two real roots if $a < 0$. It follows that $f(x)$ is increasing everywhere if $a > 0$, and its graph has a shape as in Figure 2.1.

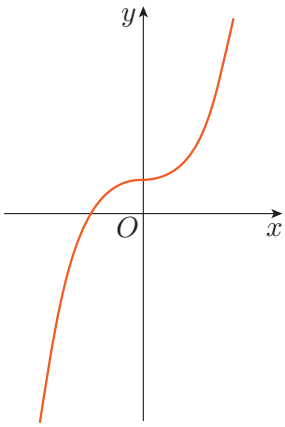
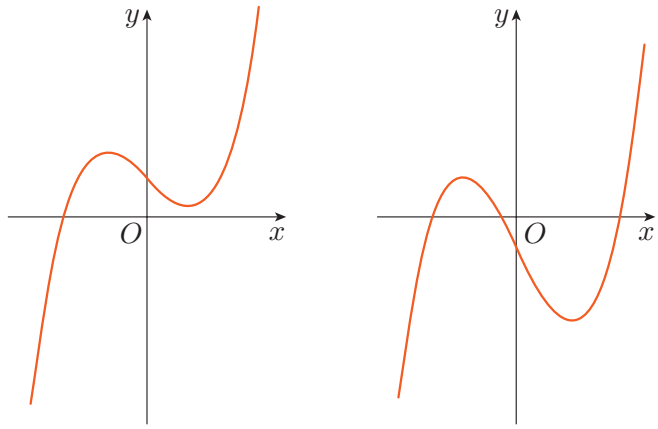


Figure 2.1 The shape of the graph of $f(x) = x^3 + ax + b$ for $a > 0$

If $a < 0$, then $f(x)$ is increasing in the intervals $(-\infty, -\sqrt{-\frac{a}{3}})$ and $(\sqrt{-\frac{a}{3}}, \infty)$ and decreasing in the interval $(-\sqrt{-\frac{a}{3}}, \sqrt{-\frac{a}{3}})$, with a local maximum at $x = -\sqrt{-\frac{a}{3}}$ and a local minimum at $x = +\sqrt{-\frac{a}{3}}$. The second derivative $f''(x) = 6x$ shows that the graph of $f(x)$ is concave down in the interval $(-\infty, 0)$ and concave up in $(0, \infty)$. Since the values of $f(x)$ approach $+\infty$ and $-\infty$ as x tends to $+\infty$ and $-\infty$, respectively, the shape of the cubic function $f(x)$ for $a < 0$ is either as in Figure 2.2(a) or as in Figure 2.2(b).



(a) (b)

Figure 2.2 Possible shapes for the graph of $f(x) = x^3 + ax + b$ for $a < 0$

We now state and prove a necessary and sufficient condition for the polynomial $f(x) = x^3 + ax + b$ over the field $\mathbb{R}$ with $4a^3 + 27b^2 \neq 0$ to have three distinct real roots.

Lemma 2.2

Let $f(x) = x^3 + ax + b$ be a cubic polynomial over $\mathbb{R}$ such that $4a^3 + 27b^2 \neq 0$. Then $f(x)$ has three real roots if $a < 0$ and $|b| < \frac{2|a|\sqrt{|a|}}{3\sqrt{3}}$, and exactly one real root otherwise.

Proof From calculus and the shape of the graph of $f(x)$ we know that the polynomial $f(x)$ over $\mathbb{R}$ has a double root if, and only if, the x-axis is a tangent line to the graph of the cubic function $f(x)$, and then the double root is precisely the point of tangency. Also, Figure 2.2 and the discussion preceding it show that if $f(x)$ has a double root, then $a < 0$ and the double root must be the point x_0 at which $f(x)$ attains its local maximum or its local minimum. This happens precisely at the point x_0 for which $f'(x_0) = 0$, that is, at $x_0 = \pm\sqrt{\frac{|a|}{3}}$ for $a < 0$. By the proof of Lemma 2.1 we know that in such a case we have $b = 2x_0^3$, or, equivalently, $b = \pm\frac{2|a|\sqrt{|a|}}{3\sqrt{3}}$.

Since the value of b represents a vertical shift of the graph of $x^3 + ax$ depicted in Figure 2.3, we conclude that $f(x)$ has three real roots if, and only if, $a < 0$ and the shift b lies in the interval $(-\frac{2|a|\sqrt{|a|}}{3\sqrt{3}}, \frac{2|a|\sqrt{|a|}}{3\sqrt{3}})$. ■

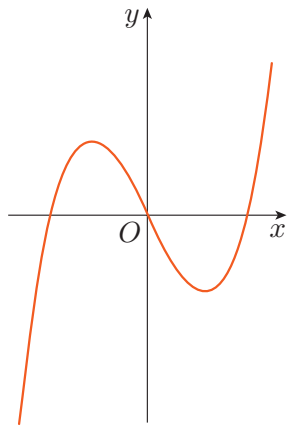


Figure 2.3 The shape of the graph of $x^3 + ax$ for $a < 0$

2.2 Elliptic curves: definition and examples

We are now ready to state one of the central definitions of this chapter.

Definition 2.3 *Elliptic curve*

Let F be a field of characteristic distinct from 2 and 3, and let $f(x) = x^3 + ax + b$ be a cubic polynomial over F such that $4a^3 + 27b^2 \neq 0$. Let $\mathcal{O}$ be a symbol, distinct from all elements of $F \times F$. The set

$$E_F(a, b) = \{\mathcal{O}\} \cup \{(x, y) \in F \times F : \ y^2 = f(x)\}$$

is called an **elliptic curve** over the field F.

Elements of an elliptic curve $E_F(a, b)$ are usually referred to as **points** on the curve. The special symbol $\mathcal{O}$ is sometimes called a **point at infinity**. At this time the symbol $\mathcal{O}$ may appear artificial; its importance will be made clear later.

Observe that if $P = (x, y)$ is a point on an elliptic curve $E_F(a, b)$, then the point with coordinates $(x, -y)$, denoted $-P$, is also a point on the same curve. Thus, P and $-P$ have the same x-coordinate but their y-coordinates differ in sign. In the special case when $y = 0$, that is, when $P = (x, 0)$ and $x \in F$ is a (simple) root of the polynomial $f(x) = x^3 + ax + b$, we have $P = -P$. If we set $\mathcal{O} = -\mathcal{O}$, the map $P \mapsto -P$ defines a bijection of $E_F(a, b)$ into itself.

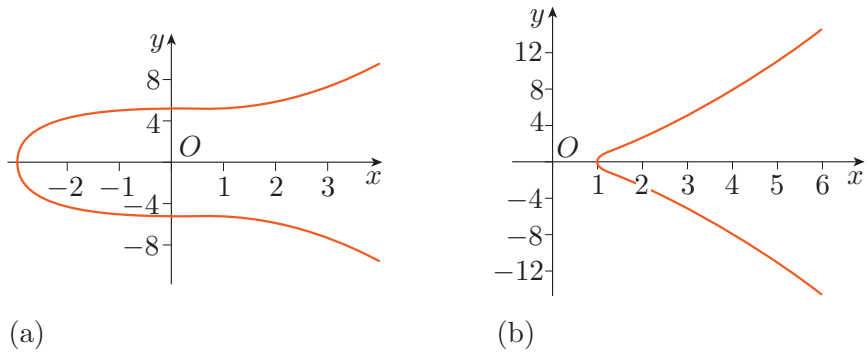
We now look at elliptic curves over a number of different fields and we discuss the possible shapes of their graphs.

Example 2.4 *Real elliptic curves*

Let $f(x) = x^3 + b$ be a polynomial over the field of real numbers, where b is a non-zero real number. The polynomial $f(x)$ has a single real root, $x_0 = \sqrt[3]{-b}$. Moreover, the square root $\sqrt{f(x)}$ is real if, and only if, $x^3 + b \geq 0$, that is, if, and only if, $x \geq x_0$. Thus, the elliptic curve $E_{\mathbb{R}}(0, b)$ contains the point $(x_0, 0)$ and, for every $x > x_0$, the pair of points $P_x = (x, \sqrt{f(x)})$ and $-P_x = (x, -\sqrt{f(x)})$, together with $\mathcal{O}$. Formally,

$$E_{\mathbb{R}}(0, b) = \{\mathcal{O}\} \cup \{(x, \pm\sqrt{x^3 + b}) : \ x \in \mathbb{R}, \ x \geq \sqrt[3]{-b}\}.$$

The graph of this kind of elliptic curve is shaped either as in the example in Figure 2.4(a) or the example in Figure 2.4(b).



(a) (b)

Figure 2.4 The elliptic curves: (a) $E_{\mathbb{R}}(0, 27)$, that is, $y^2 = x^3 + 27$; (b) $E_{\mathbb{R}}(0, -1)$, that is, $y^2 = x^3 - 1$

Inspired by Example 2.4, we will now attempt to study a general elliptic curve $E_{\mathbb{R}}(a, b) = \{\mathcal{O}\} \cup \{(x, y) \in \mathbb{R} \times \mathbb{R} : \ y^2 = x^3 + ax + b\}$ corresponding to a polynomial $f(x) = x^3 + ax + b$ over $\mathbb{R}$, with $4a^3 + 27b^2 \neq 0$ and $a \neq 0$. Note that, up to the point $\mathcal{O}$, graphing $E_{\mathbb{R}}(a, b)$ is equivalent to graphing the curve $|y| = \sqrt{x^3 + ax + b}$.

If $f(x)$ has exactly one real root x_0, then the domain of the function $y = \sqrt{x^3 + ax + b}$ is the interval $[x_0, \infty)$. The graph of $y = \sqrt{x^3 + ax + b}$, and hence the graph of $E_{\mathbb{R}}(a, b)\backslash\{\mathcal{O}\}$, in the open interval (x_0, ∞) is obtained by taking $\pm$ the square root of the values on the part of the graph of $f(x)$ that lies above the x-axis.

Let us now discuss the case when $f(x) = x^3 + ax + b$ with $4a^3 + 27b^2 \neq 0$ has exactly 3 real roots, say, $x_1 < x_2 < x_3$. By Lemma 2.2, this happens if, and only if, $a < 0$ and $|b| < \frac{2|a|\sqrt{|a|}}{3\sqrt{3}}$. In this case the domain of the curve $|y| = \sqrt{x^3 + ax + b}$ is $[x_1, x_2] \cup [x_3, \infty)$ and the curve has two components. Its graph is again obtained by taking $\pm$ the square root of the values on the two parts of the graph of $f(x)$ that lie above the x-axis.

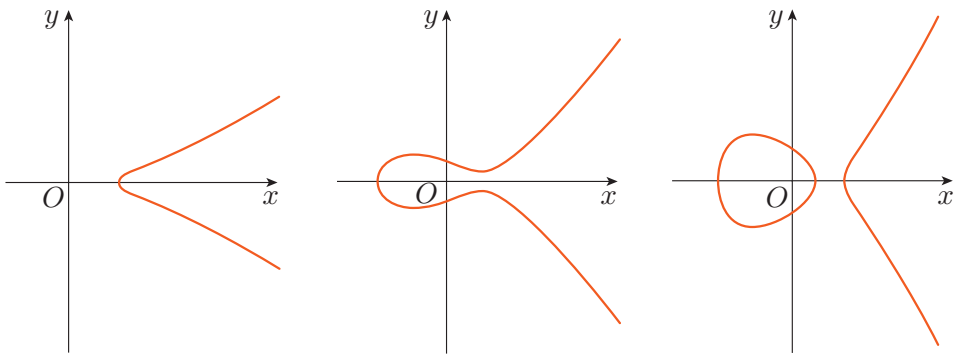
The three typical shapes of elliptic curves $E_{\mathbb{R}}(a,b)$ are depicted in Figures 2.5(a), 2.5(b) and 2.5(c) in the cases

(i) $b < 0 < a$,

(ii) $a < 0$ and $b > \frac{2|a|\sqrt{|a|}}{3\sqrt{3}}$, and

(iii) $a < 0$ and $|b| < \frac{2|a|\sqrt{|a|}}{3\sqrt{3}}$.

In all these situations, observe that the bijection $P \mapsto -P$ of any elliptic curve over $\mathbb{R}$ into itself shows as a reflection of the graph in the x-axis.



(a) (b) (c)

Figure 2.5 The shape of the graph of an elliptic curve $E_{\mathbb{R}}(a,b)$ where: (a) $b < 0 < a$; (b) $a < 0$ and $b > \frac{2|a|\sqrt{|a|}}{3\sqrt{3}}$; (c) $a < 0$ and $|b| < \frac{2|a|\sqrt{|a|}}{3\sqrt{3}}$

Example 2.5 *Complex elliptic curves*

Let $\mathbb{C}$ denote the field of complex numbers, and let $f(x) = x^3 + b$, where $b \neq 0$. What does the corresponding elliptic curve $E_{\mathbb{C}}(0,b)$ look like?

Let $\omega = e^{\frac{2\pi i}{3}} = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$. Then the three roots of $f(x)$ are

$$x_j = \omega^j \sqrt[3]{-b} \text{ for } j = 0, 1, 2.$$

It follows that $E_{\mathbb{C}}(0,b)$ contains the three points $(x_j, 0)$ for $j = 0, 1, 2$. For $x \in \mathbb{C}$ such that $x \notin \{x_0, x_1, x_2\}$, we have that $f(x) \neq 0$ and the equation $y^2 = f(x)$ has two distinct complex roots. If we denote one of the roots by $\sqrt{f(x)}$, then every $x \in \mathbb{C}\backslash\{x_0, x_1, x_2\}$ gives rise to two distinct points $(x, \sqrt{f(x)})$ and $(x, -\sqrt{f(x)})$ in $E_{\mathbb{C}}(0,b)$. In summary,

$$E_{\mathbb{C}}(0,b) = \{\mathcal{O}\} \cup \{(x, \pm\sqrt{x^3 + b}) : x \in \mathbb{C}\}.$$

Obtaining a graph of $E_{\mathbb{C}}(0,b)$ is a difficult task. Nevertheless, more advanced methods than the ones at our disposal show that $E_{\mathbb{C}}(0,b)$ can be represented in $\mathbb{R}^3$ as the set of points of a torus, an object that looks like the inner tube of a tyre.

Example 2.6 *Rational elliptic curves*

We now consider elliptic curves over the field $\mathbb{Q}$ of rational numbers. Let $f(x) = x^3 + ax + b$ be such that $a, b \in \mathbb{Q}$ and $4a^3 + 27b^2 \neq 0$. Besides the exceptional point $\mathcal{O}$, an elliptic curve $E_{\mathbb{Q}}(a, b)$ consists of ordered pairs (x, y) of rational numbers such that $y^2 = x^3 + ax + b$. This means that for (x, y) to be a point on $E_{\mathbb{Q}}(a, b)$ for some rational number x, the square root $y = \sqrt{x^3 + ax + b}$ must be a rational number as well.

This is a very restrictive requirement and its full understanding is one of the major open problems in contemporary mathematics. To illustrate the difficulties, we list four examples, on which we comment below:

(i) $E_{\mathbb{Q}}(1, -47)$ consists just of the point at infinity, $\mathcal{O}$

(ii) $E_{\mathbb{Q}}(1, 2) = \{\mathcal{O}, (-1, 0), (1, 2), (1, -2)\}$

(iii) $E_{\mathbb{Q}}(1, 1)$ is infinite and can be 'generated' by one point

(iv) $E_{\mathbb{Q}}(1, 9)$ is infinite and can be 'generated' by two points but not by one.

Example (i) tells us that the equation $y^2 = x^3 + x - 47$ has no rational solution, while example (ii) tells us that the equation $y^2 = x^3 + x + 2$ has just 3 rational solutions.

Example (iii) is more exciting, as the equation $y^2 = x^3 + x + 1$ has an infinite number of rational solutions. The surprise, however, comes from the first 14 rational solutions (x, y) in their simplest form:

$$(0, \pm 1)\,,\ (72, \pm 611)\,,\ \left(\frac{1}{4}, \pm\frac{9}{8}\right),\ \left(\frac{-287}{1296}, \pm\frac{40\,879}{46\,656}\right),\ \left(\frac{43\,992}{82\,369}, \pm\frac{30\,699\,397}{23\,639\,903}\right),$$
$$\left(\frac{26\,862\,913}{1\,493\,284}, \pm\frac{139\,455\,877\,527}{1\,824\,793\,048}\right),\ \left(-\frac{3\,596\,697\,936}{8\,760\,772\,801}, \pm\frac{591\,456\,591\,665\,497}{819\,999\,573\,400\,799}\right).$$

The sense in which all the points on the rational elliptic curve $E_{\mathbb{Q}}(1, 1)$ are 'generated' by a single point will be explained later: we will see that every elliptic curve is, at the same time, an abelian group with an operation of addition, which is derived from certain geometric properties of the graphs of these curves. Moreover, the abelian group defined on $E_{\mathbb{Q}}(1, 1)$ turns out to be isomorphic to the additive group of the integers, $(\mathbb{Z}, +)$, which, as you know, is generated by the single element 1.

In contrast with this, the elliptic curve $E_{\mathbb{Q}}(1, 9)$ in example (iv) turns out to be isomorphic, as an abelian group, to the direct product $\mathbb{Z} \times \mathbb{Z}$. This group can be generated by two generators, but not by one. Complete proofs of these facts are well beyond the scope of this module.

Exercise 2.2

Find all the points (x, y) on the rational elliptic curve $E_{\mathbb{Q}}(1, 9)$ such that x, y are integers and $0 \leq x \leq 10$.

This section concludes with an example of a family of elliptic curves over the finite field GF_p where p is any odd prime such that $p \equiv 2 \pmod 3$.

Example 2.7 *Elliptic curves over finite fields*

Let p be an arbitrary odd prime such that $p \equiv 2 \pmod 3$ and let GF_p be the finite field of order p. For an arbitrary non-zero $b \in GF_p$ we consider the elliptic curve $E_{GF_p}(0, b)$ defined by the cubic polynomial $f(x) = x^3 + b$ over GF_p.

Recall that the multiplicative group GF_p^* of GF_p has order $p - 1$ and it is cyclic. Our assumption on p implies that $p - 1$ is not a multiple of 3, which in turn implies that GF_p^* contains no element of order 3. We prove that in this case for any $c \in GF_p$ the equation $z^3 = c$ has a unique solution $z \in GF_p$.

This statement is true for $c = 0$. To prove it for all $c \neq 0$, it is sufficient to show that the map $z \mapsto z^3$ is a bijection of the set GF_p^* into itself. Since GF_p^* is finite, it is sufficient to show that the map $z \mapsto z^3$ is injective on GF_p^*. Assume that $z_1^3 = z_2^3$ for some $z_1, z_2 \in GF_p^*$. Then $(z_2^{-1} z_1)^3 = 1$, and since GF_p^* contains no element of order 3, we must have $z_2^{-1} z_1 = 1$, and hence $z_2 = z_1$.

Any injective map of a finite set into itself is a bijection.

Thus, if p is odd and $p \equiv 2 \pmod 3$, for every $c \in GF_p$ there is a unique $z \in GF_p$ such that $z^3 = c$; we will denote this element z by $\sqrt[3]{c}$ as usual.

We can now determine the elliptic curve $E_{GF_p}(0, b)$ by listing all ordered pairs (x, y) of elements of GF_p such that $y^2 = x^3 + b$.

Firstly, the point $(\sqrt[3]{-b}, 0)$ is on the curve. Secondly, for any $x \in GF_p$ such that $x \neq \sqrt[3]{-b}$, the map $\theta\colon\ x \mapsto x^3 + b$ is, by a similar argument to that for $z \mapsto z^3$, a bijection from the set $GF_p \backslash \{\sqrt[3]{-b}\}$ onto GF_p^*. In order to determine y, we must be able to take the square root of $x^3 + b$, and this can be done if, and only if, $x^3 + b$ is a square in GF_p^*.

So let S denote the set of all the elements $x \in GF_p \backslash \{\sqrt[3]{-b}\}$ such that $x^3 + b$ is a square in GF_p^*. Since the map θ is a bijection and GF_p^* contains exactly $\frac{p-1}{2}$ squares by Proposition 1.4 of Book C, Chapter 10, we have $|S| = \frac{p-1}{2}$. Finally, for each $x \in S$ there are two values of the square root of $x^3 + b$, for which we use the customary notation $\pm\sqrt{x^3 + b}$. It follows that, for any odd prime $p \equiv 2 \pmod 3$ and any $b \in GF_p^*$ we have

$$E_{GF_p}(0, b) = \{\mathcal{O}\} \cup \{(\sqrt[3]{-b}, 0)\} \cup \{(x, \pm\sqrt{x^3 + b})\colon\ x \in S\}\,;$$

in particular, any such elliptic curve contains exactly $p + 1$ points.

Elliptic curves of the kind considered in Example 2.7 can be graphed, but since the curves are finite, their graphs appear as finite collections of isolated points.

Consider for instance the elliptic curve $E_{GF_{11}}(0,1)$ without the point $\mathcal{O}$. For our calculations, let us identify GF_{11} with the set $\{0, \pm1, \pm2, \pm3, \pm4, \pm5\}$. To follow the method outlined in Example 2.7, we find that $\sqrt[3]{-1} = -1$, and then we work out the set of squares in GF_{11}^* and the values of $x^3 + 1$ as x ranges over the elements of $GF_{11} \setminus \{-1\}$.

Table 2.1 The squares in GF_{11}^*

y	±1	±2	±3	±4	±5
y^2	1	4	-2	5	3

Table 2.2 The values of $x^3 + 1$ in $GF_{11} \setminus \{-1\}$

x	0	1	2	3	4	5	$6 \equiv -5$	$7 \equiv -4$	$8 \equiv -3$	$9 \equiv -2$
$x^3 + 1$	**1**	2	**-2**	-5	-1	**5**	-3	**3**	-4	**4**

Table 2.1 shows that the set of squares in GF_{11}^* is $\{1, -2, 3, 4, 5\}$. In Table 2.2, the elements that are squares have been highlighted in blue. We infer that $S = \{0, 2, -2, -4, 5\}$. Therefore

$$E_{GF_{11}}(0,1) = \{\mathcal{O}, (0, \pm1), (2, \pm3), (5, \pm4), (7, \pm5), (9, \pm2), (10, 0)\}.$$

A graph of $E_{GF(11)}(0,1)\setminus\{\mathcal{O}\}$ is in Figure 2.6.

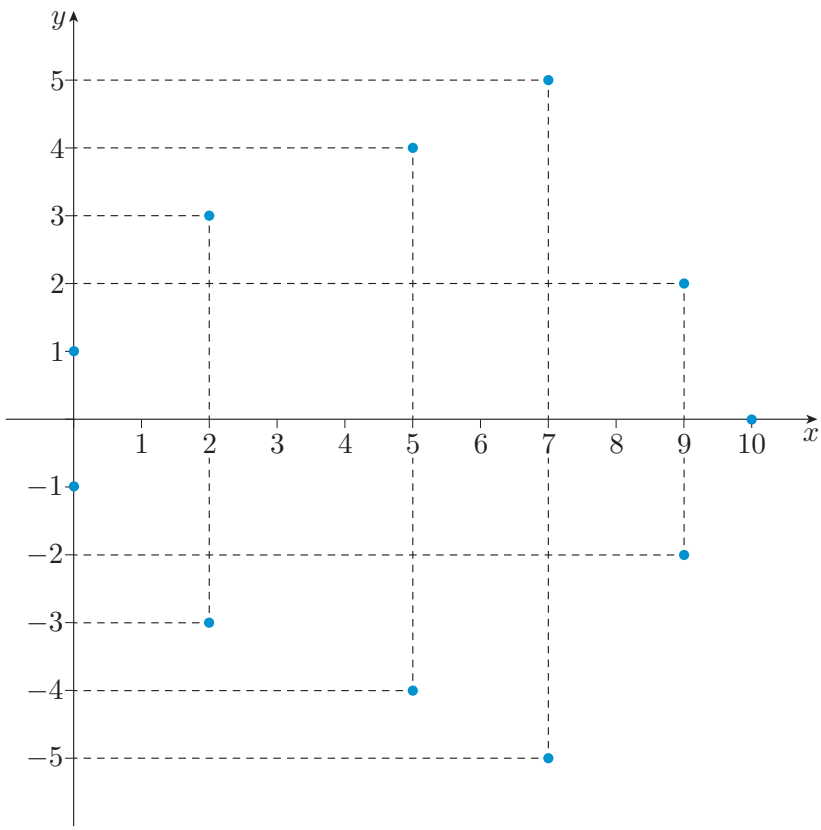


Figure 2.6 A graph of the elliptic curve $E_{GF_{11}}(0,1)\setminus\{\mathcal{O}\}$

Exercise 2.3

Draw the elliptic curve $E_{GF_{13}}(0, 2)\backslash\{\mathcal{O}\}$.

2.3 Elliptic curves as abelian groups

We now introduce an operation on the points of an elliptic curve that makes the curve into an abelian group. In the case of elliptic curves over the field of real numbers, the operation can be defined in geometric terms by considering (straight) lines that intersect the curve. In order to generalise this idea to arbitrary fields, we first generalise the notion of a line over a field.

Definition 2.8 *Line with slope*

Let F be a field and let $\mathcal{O} \notin F \times F$ be the point at infinity.

(a) For any chosen $c, d \in F$, a **line with slope** c is the set

$$L(c, d) = \{(x, y) \in F \times F : y = cx + d\}.$$

(b) For any $x_0 \in F$, a **slopeless line** is the set

$$L(x_0) = \{\mathcal{O}\} \cup \{(x, y) \in F \times F : x = x_0\}.$$

To simplify the terminology, the term **line over** F will be used to refer to both lines with slope and slopeless lines.

Lines with slope are a generalisation of the real lines $y = cx + d$. Slopeless lines over arbitrary fields are also generalisations of the real lines $x = x_0$ parallel to the y-axis, except that we have defined slopeless lines to include $\mathcal{O}$, our mysterious point at infinity. In particular, by definition, any two distinct slopeless lines intersect at exactly one point, namely, $\mathcal{O}$.

We can now also generalise the notion of a tangent line to an elliptic curve over a field. We take inspiration in the field $\mathbb{R}$ again.

Suppose that $y^2 = x^3 + ax + b$ defines an elliptic curve $E_{\mathbb{R}}(a, b)$ over $\mathbb{R}$ and let $P = (x_0, y_0)$ be a point on the graph of this curve. The slope of the tangent line to the curve at P is found by implicit differentiation, which you will have met in your previous studies. Differentiating $y^2 = x^3 + ax + b$ with respect to x gives

$$2yy'(x) = 3x^2 + a,$$

and evaluating at P gives

$$2y_0y'(x_0) = 3x_0^2 + a. \tag{5}$$

It follows that the slope of the tangent line to our curve at P is undefined if $y_0 = 0$. If $y_0 \neq 0$, however, the slope c_0 of the tangent line is equal to $y'(x_0)$ calculated from (5), that is,

$$c_0 = \frac{3x_0^2 + a}{2y_0}. \tag{6}$$

Thus, if $y_0 \neq 0$, the equation of the tangent line at P is $y - y_0 = c_0(x - x_0)$, or

$$y = c_0 x + d_0 \text{ where } d_0 = y_0 - c_0 x_0. \tag{7}$$

Substituting for c_0 from (6) into the equation for d_0 in (7), using $y_0^2 = x_0^3 + ax_0 + b$ and simplifying give

$$d_0 = \frac{-x_0^3 + ax_0 + 2b}{2y_0}. \tag{8}$$

If $y_0 = 0$, the tangent line at P is slopeless and has equation $x = x_0$. Equivalently, $L(c_0, d_0)$, where c_0 and d_0 are as in (6) and (8) respectively, is the tangent line to the elliptic curve $E_{\mathbb{R}}(a, b)$ at the point (x_0, y_0) if $y_0 \neq 0$, and $L(x_0)$ is the tangent to $E_{\mathbb{R}}(a, b)$ at the point (x_0, y_0) if $y_0 = 0$.

All these considerations hold for elliptic curves over the field $\mathbb{R}$ of real numbers. We extend these ideas to arbitrary fields in the next definition.

Definition 2.9 *Tangent line with slope*

Let $E_F(a, b)$ be an elliptic curve over a field F of characteristic distinct from 2 and 3, and let $P = (x_0, y_0)$ be a point on this curve.

(a) If $y_0 \neq 0$, the line $L(c_0, d_0)$, where

$$c_0 = \frac{3x_0^2 + a}{2y_0} \quad \text{and} \quad d_0 = \frac{-x_0^3 + ax_0 + 2b}{2y_0},$$

is said to be the **tangent line with slope** c_0 to the curve at P.

(b) If $y_0 = 0$, the line $L(x_0)$ is said to be the **slopeless tangent line** to $E_F(a, b)$ at P.

Again, to simplify the terminology, we will simply speak about **tangent lines** to an elliptic curve.

We now prove a basic auxiliary result relating elliptic curves to lines, which will enable us to introduce addition of points of an elliptic curve.

Lemma 2.10

Let $E_F(a, b)$ be an elliptic curve over a field F of characteristic distinct from 2 and 3.

(a) Let $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$ be points on $E_F(a, b)$ distinct from $\mathcal{O}$ and such that $P_1 \neq \pm P_2$. Then the (unique) line through P_1 and P_2 is $L(c, d)$, where

$$c = \frac{y_2 - y_1}{x_2 - x_1} \quad \text{and} \quad d = \frac{y_1 x_2 - y_2 x_1}{x_2 - x_1}.$$

This line intersects the elliptic curve at the point $\pi(P_1, P_2) = (x_3, y_3)$, where $x_3 = c^2 - x_1 - x_2$ and $y_3 = cx_3 + d$.

(b) Let $P_0 = (x_0, y_0)$ be a point on $E_F(a, b)$ such that $y_0 \neq 0$. Then the tangent line $L(c_0, d_0)$, where c_0 and d_0 are as in Definition 2.9, intersects the curve $E_F(a, b)$ in the point $\pi'(P_0) = (x', y')$, where $x' = c_0^2 - 2x_0$ and $y' = c_0 x' + d_0$.

Proof

(a) Let P_1 and P_2 be as in our statement. Since $x_1 \neq x_2$, the unique line through P_1 and P_2 over F has equation

$$y - y_1 = c(x - x_1)$$

exactly as in calculus, with slope

$$c = \frac{y_2 - y_1}{x_2 - x_1}.$$

Equivalently, the line has equation $y = cx + d$, where $d = y_1 - cx_1$. Substituting for c yields

$$d = \frac{y_1 x_2 - y_2 x_1}{x_2 - x_1}.$$

To calculate any other intersection points of the line $L(c, d)$ of equation $y = cx + d$ with our elliptic curve of equation $y^2 = x^3 + ax + b$, we eliminate y, which gives the polynomial equation

$$(cx + d)^2 = x^3 + ax + b,$$

or, equivalently,

$$x^3 - c^2x^2 + (a - 2cd)x + (b - d^2) = 0.$$

This cubic equation has three roots (possibly repeated). By our assumption, however, we already know two distinct roots of this equation, namely, x_1 and x_2. If we denote the third root by x_3, we have

$$x^3 - c^2x^2 + (a - 2cd)x + (b - d^2) = (x - x_1)(x - x_2)(x - x_3). \quad (9)$$

Comparing the coefficients of x^2 on both sides of equation (9) gives $x_1 + x_2 + x_3 = c^2$ and hence $x_3 = c^2 - x_1 - x_2$. If $\pi(P_1, P_2) = (x_3, y_3)$ is the point of intersection of $L(c, d)$ and $E_F(a, b)$, and the x-coordinate is equal to x_3, then $y_3 = cx_3 + d$. This proves the first part of our lemma.

(b) By Definition 2.9, the tangent line to the curve at P_0 is $L(c_0, d_0)$, where

$$c_0 = \frac{3x_0^2 + a}{2y_0}, \quad d_0 = \frac{-x_0^3 + ax_0 + 2b}{2y_0}.$$

To calculate any other points of intersection of the line $L(c_0, d_0)$ with the elliptic curve, we again look for simultaneous solutions to the equations $y = c_0x + d_0$ and $y^2 = x^3 + ax + b$. Eliminating y yields

$$(c_0x + d_0)^2 = x^3 + ax + b,$$

or, equivalently,

$$x^3 - c_0^2x^2 + (a - 2c_0d_0)x + (b - d_0^2) = 0.$$

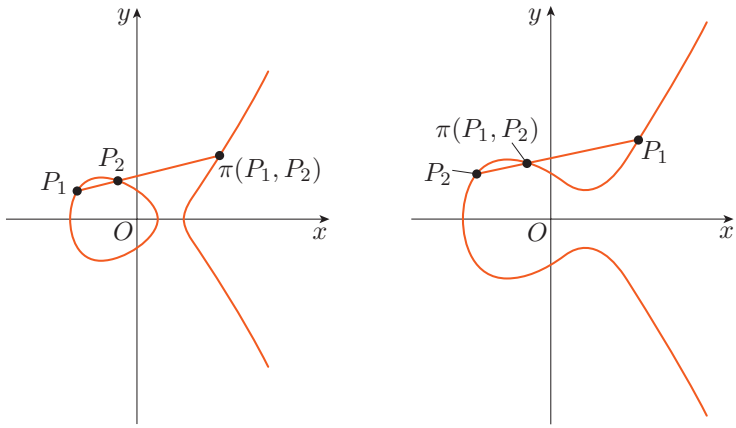
If the underlying field is the field of real numbers $\mathbb{R}$, a point of tangency is a root of the last equation of multiplicity at least two. This is also true over a finite field, although we shall not give a proof here. So, in general, since $L(c_0, d_0)$ is a tangent line at x_0, we know that x_0 is a root of multiplicity at least two. Thus if we denote the remaining root by x_3, we obtain

$$(x - x_0)^2(x - x_3) = x^3 - c_0^2x^2 + (a - 2c_0d_0)x + (b - d_0^2).$$

Comparing the coefficients of x^2 gives $x_3 = c_0^2 - 2x_0$, and so $y_3 = c_0x_3 + d_0$. The substitution $x_3 = x'$ and $y_3 = y'$ gives the required coordinates for the point of intersection. ■

We note that the points $\pi(P_1, P_2)$ and $\pi'(P_0)$ in Lemma 2.10 are not necessarily distinct from one of P_1, P_2 and from P_0, respectively.

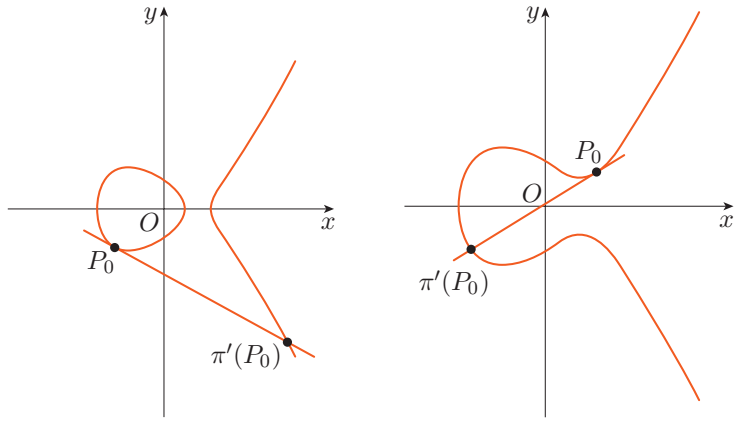
Two possible configurations for P_1, P_2 and $\pi(P_1, P_2)$ are depicted in Figure 2.7.



(a) (b)

Figure 2.7 Two possible configurations for P_1, P_2 and $\pi(P_1, P_2)$

Similarly, two typical situations that one may encounter in determining $\pi'(P_0)$ are given in Figure 2.8.



(a) (b)

Figure 2.8 Two possible configurations for P_0 and $\pi'(P_0)$

Worked Exercise 2.11 *Computing $\pi(P_1, P_2)$ and $\pi'(P_0)$*

Consider the elliptic curve $E_{GF_{19}}(1,1)$ corresponding to $y^2 = x^3 + x + 1$ over GF_{19}, together with the points $P_1 = (0,1)$, $P_2 = (5,6)$ and $P_0 = (9,-6)$ on this curve. Determine the points $\pi(P_1, P_2)$ and $\pi'(P_0)$.

Solution

To calculate $\pi(P_1, P_2)$ we use part (a) of Lemma 2.10 for the values $a = b = 1$, $(x_1, y_1) = (0,1)$ and $(x_2, y_2) = (5,6)$. We obtain

$$c = \frac{6-1}{5-0} = 1 \quad \text{and} \quad d = \frac{1 \times 5 - 6 \times 0}{5-0} = 1,$$

where the calculations are in GF_{19}, and

$$x_3 = 1^2 - 5 - 0 = -4, \quad y_3 = 1 \times (-4) + 1 = -3,$$

again in GF_{19}. It follows that $\pi(P_1, P_2) = (-4, -3)$.

Similarly, to compute $\pi'(P_0)$ we follow part (b) of Lemma 2.10 with $a = b = 1$ and $(x_0, y_0) = (9, -6)$. To determine c_0, we must evaluate the quotient

$$c_0 = \frac{3 \times 9^2 + 1}{2 \times (-6)} = \frac{244}{-12}$$

in GF_{19}, that is, we must solve the linear congruence

$$-12c_0 \equiv 244 \pmod{19}.$$

Since $244 \equiv 16 \pmod{19}$ and $-12 \equiv 7 \pmod{19}$, the strategy for solving linear congruences in Book A, Chapter 3, Subsection 3.3 tells us that this congruence is equivalent to

$$7c_0 \equiv 16 \pmod{19}.$$

Multiplying each side by 3 modulo 19 gives

$$2c_0 \equiv 10 \pmod{19},$$

which gives $c_0 = 5$. Similarly, finding

$$d_0 = \frac{-9^3 + 1 \times 9 + 2 \times 1}{2 \times (-6)} = \frac{-718}{-12} = \frac{359}{6}$$

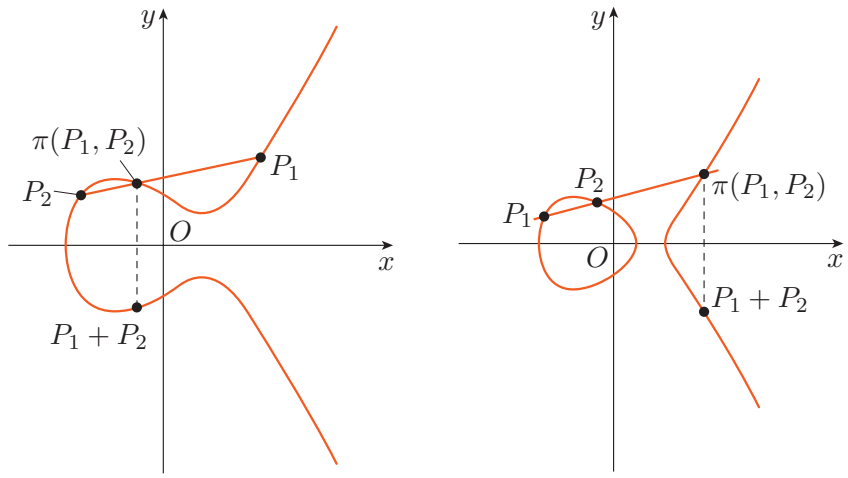
in GF_{19} is equivalent to solving the linear congruence

$$6d_0 \equiv 359 \pmod{19}.$$

Again, using the strategy given in Book A, Chapter 3, Subsection 3.3 gives $d_0 = 6$. We can now work out $x' = 5^2 - 2 \times 9 \equiv 7 \pmod{19}$ and $y' = 5 \times 7 + 6 \equiv 3 \pmod{19}$. Therefore $\pi'(P_0) = (7, 3)$.

Lemma 2.10 will enable us to define an operation of addition of points of an elliptic curve. To help intuition, we first give an informal description of the operation when the underlying field is the field of real numbers.

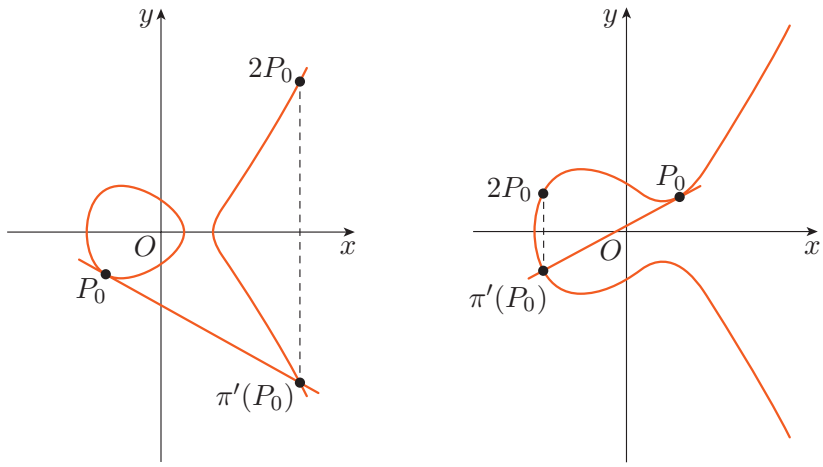
Suppose that P_1 and P_2 are two distinct points on an elliptic curve $E_{\mathbb{R}}(a, b)$ and suppose that the unique line through P_1 and P_2 intersects the curve in a third point $P_3 = \pi(P_1, P_2)$ distinct from P_1, P_2. We will then define $P_1 + P_2$ to be equal to $-P_3$. Two examples are illustrated in Figure 2.9.



(a) (b)

Figure 2.9 Two examples of addition on an elliptic curve

If P_0 is a point on $E_{\mathbb{R}}(a, b)$ such that the tangent line to the curve at P_0 is not vertical and intersects the curve in a point $\pi'(P_0)$ distinct from P_0, then we define $P_0 + P_0 = -\pi'(P_0)$. Two examples of 'doubling' are illustrated in Figure 2.10.



(a) (b)

Figure 2.10 Two examples of doubling on an elliptic curve

Of course, the above examples are just two instances of addition. The general definition, which we are about to give, must account for more cases. We use the notation introduced in Lemma 2.10.

Definition 2.12 *Addition of points on an elliptic curve*

Let F be a field of characteristic distinct from 2 and 3, and let $E_F(a,b)$ be an elliptic curve over F. Let P, P_0, P_1 and P_2 be arbitrary points on $E_F(a,b)$ distinct from $\mathcal{O}$, with $P_1 \neq P_2$. We define a binary operation on $E_F(a,b)$ as follows:

(a) $\mathcal{O} + \mathcal{O} = \mathcal{O}$

(b) $P + \mathcal{O} = \mathcal{O} + P = P$

(c) $P + (-P) = \mathcal{O}$

(d) if P_0 has non-zero y-coordinate, then $2P_0 = P_0 + P_0 = -\pi'(P_0)$

(e) if P_1 and P_2 are such that $P_1 \neq \pm P_2$, then $P_1 + P_2 = -\pi(P_1, P_2)$.

Worked Exercise 2.13 *Computing $P_1 + P_2$ and $2P_0$*

Consider again the elliptic curve $E_{GF_{19}}(1,1)$ from Worked Exercise 2.11 and the three points $P_1 = (0,1)$, $P_2 = (5,6)$ and $P_0 = (9,-6)$ on the curve. Find the points $P_1 + P_2$ and $2P_0 = P_0 + P_0$.

Solution

By parts (e) and (d) of Definition 2.12 we have $P_1 + P_2 = -\pi(P_1, P_2)$ and $2P_0 = -\pi'(P_0)$. In Worked Exercise 2.11 we saw that $\pi(P_1, P_2) = (-4,-3)$ and $\pi'(P_0) = (7,3)$. It follows that $P_1 + P_2 = -(-4,-3) = (-4,3)$ and $2P_0 = -(7,3) = (7,-3)$.

The surprising feature of the operation of addition introduced in Definition 2.12 is that it makes an elliptic curve into an abelian group! The identity element of the group is our mysterious special point at infinity, $\mathcal{O}$, which explains its importance.

Proposition 2.14

Let F be a field of characteristic distinct from 2 and 3, let $E = E_F(a,b)$ be an elliptic curve over F, and let $+$ be the binary operation on E introduced in Definition 2.12. Then $(E,+)$ is an abelian group with identity element $\mathcal{O}$. The inverse of a point P is the point $-P$.

Proof We first address a fine point – namely, we need to check that the operation $+$ is well defined. By Definition 2.12, this amounts to checking that the points $\pi(P_1, P_2)$ and $\pi'(P_0)$ are uniquely defined. This is clear for $\pi(P_1, P_2)$, since this point is uniquely defined by part (a) of Lemma 2.10 whenever $P_1 \neq \pm P_2$.

The point $\pi'(P_0)$ is uniquely defined by part (b) of Lemma 2.10 whenever $P_0 = (x_0, y_0)$ is such that $y_0 \neq 0$. Note that if a point P has zero y-coordinate, then we have $P = -P$, and $P + P = \mathcal{O}$, by Definition 2.12. We conclude that the operation $+$ is indeed well defined.

Next we prove that $(E, +)$ is an abelian group. From the fact that $\pi(P_1, P_2) = \pi(P_2, P_1)$ and from Definition 2.12 it follows that the operation $+$ is commutative. Also, $\mathcal{O}$ is the identity element by Definition 2.12(b), and the inverse of a point $P \in E$ is $-P$ by Definition 2.12(c).

The only remaining issue is associativity of the operation $+$. However, the proof that this operation is associative either uses results that are beyond the scope of this module or requires a level of calculation where it is best to use a computer. This is why we omit this last part of the proof. ■

You may have been wondering about the reason for our assumption $4a^3 + 27b^2 \neq 0$ in Definition 2.3, where we introduced elliptic curves. By Lemma 2.1, for fields F of characteristic distinct from 2 and 3 the inequality $4a^3 + 27b^2 \neq 0$ implies that the polynomial $f(x) = x^3 + ax + b$ over F has no multiple roots. So, what would go wrong with our theory if we allowed polynomials $f(x) = x^3 + ax + b$ with a multiple root?

Suppose that $f(x) = x^3 + ax + b$ has a root x_0 of multiplicity 2 and a simple root $x_1 \neq x_0$, that is, $f(x) = (x - x_0)^2(x - x_1)$. Consider the points $P_1 = (x_1, y_1) = (x_1, 0)$ and $P_2 = (x_2, y_2) = (x_0, 0)$ on the corresponding elliptic curve $E_F(a, b)$. We show that in such a case the operation $+$ would not be associative (this is one of the numerous special cases one would have to go through in proving associativity in Proposition 2.14).

Indeed, when computing $\pi(P_1, P_2)$ by part (a) of Lemma 2.10 we would have $c = d = 0$, $y_3 = 0$ and $x_3 = -x_1 - x_2$, or, equivalently, $x_0 + x_1 + x_3 = 0$. Since x_3 is now a root of $f(x)$, the left-hand side of the last equation is the sum of the three roots of $f(x)$. Since we assumed x_0 to have multiplicity 2, $x_3 = x_0$. It follows that $-\pi(P_1, P_2) = -(x_0, 0) = (x_0, 0) = P_2$, and so by Definition 2.12 we would have $P_1 + P_2 = P_2$. Observe that by the same definition we have $P_2 + P_2 = \mathcal{O}$ since P_2 has zero y-coordinate. But then Definition 2.12 would give

$$(P_1 + P_2) + P_2 = P_2 + P_2 = \mathcal{O},$$

while

$$P_1 + (P_2 + P_2) = P_1 + \mathcal{O} = P_1,$$

which violates associativity.

Observe that a contradiction already follows from the equation $P_1 + P_2 = P_2$: if we assume that $(E, +)$ is a group, we can use the cancellation law and cancel P_2 on both sides, obtaining the contradictory statement $P_1 = \mathcal{O}$. But if we were to prove Proposition 2.14 systematically as indicated above, we would only discover the contradiction when checking associativity.

If $f(x) = x^3 + ax + b$ had a root x_0 of multiplicity 3, then we would have $x^3 + ax + b = (x - x_0)^3$. Comparing coefficients for x^2 would quickly give $x_0 = 0$, so that $f(x) = x^3$ with $a = b = 0$. In this case a similar contradiction as above can be obtained for the points $P_1 = (0, 0)$ and $P_2 = (1, 1)$.

This is a good place to clarify what happens to the points $P_1 = (x_1, 0)$, $P_2 = (x_2, 0)$ and $P_3 = (x_3, 0)$ if $f(x)$ has three distinct roots x_1, x_2 and x_3 in F. If we use Lemma 2.10(a) and argue as above, we find that $P_1 + P_2 = P_3$. Since $P_j = -P_j$ for $j \in \{1, 2, 3\}$, we also have $P_2 + P_3 = P_1$ and $P_3 + P_1 = P_2$. We see that, in this case, the set $\{\mathcal{O}, P_1, P_2, P_3\}$ forms a subgroup of $(E, +)$ isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$.

We conclude with a remark. From now on we will identify an elliptic curve $E = E_F(a, b)$ with the corresponding abelian group $(E, +)$. Also, as usual when working with abelian groups, if P is an element of an elliptic curve $(E, +)$, we will write $2P$ for $P + P$, $3P$ for $P + P + P$, and so on.

2.4 Examples of elliptic curves as abelian groups

This subsection is intended to provide practice of calculations in elliptic curves regarded as abelian groups. Remember that when we apply Lemma 2.10 to an elliptic curve over the finite field GF_p, all the calculations – in particular of c_0, d_0, c and d – are modulo p.

Worked Exercise 2.15 *The rational elliptic curve $E_{\mathbb{Q}}(1, 2)$*

Describe the group $(E_1, +)$ for the rational elliptic curve $E_1 = E_{\mathbb{Q}}(1, 2) = \{\mathcal{O}, (-1, 0), (1, \pm 2)\}$ from Example 2.6.

Solution

Since E_1 has four elements and there are only two groups of order 4, the group $(E_1, +)$ is either isomorphic to $\mathbb{Z}_4$ or to $\mathbb{Z}_2 \times \mathbb{Z}_2$ by Theorem 3.2 of Book B, Chapter 7. Let us try to compute the element $2P_0 = P_0 + P_0$ for $P_0 = (1, 2)$. Lemma 2.10(b) with $a = 1$, $b = 2$, $x_0 = 1$ and $y_0 = 2$ gives $c_0 = 1$, $d_0 = 1$, $x' = -1$ and $y' = 0$. It follows that $\pi'(P_0) = (x', y') = (-1, 0)$. Applying Definition 2.12 to $P_0 + P_0$ gives $2P_0 = -\pi'(P_0) = (-1, 0)$.

Since $2P_0 \neq \mathcal{O}$, the element P_0 does not have order 2 in the group $(E_1, +)$. In this rather special case, this finding already determines the group: as every non-identity element of $\mathbb{Z}_2 \times \mathbb{Z}_2$ has order 2, our group $(E_1, +)$ must be isomorphic to $\mathbb{Z}_4$. The reader is invited to check that $3P_0 = 2P_0 + P_0 = (1, -2)$, and so P_0 is a generator of $(E_1, +) \simeq \mathbb{Z}_4$.

Example 2.16 *The rational elliptic curve $E_{\mathbb{Q}}(1,1)$*

Another rational elliptic curve considered in Example 2.6 was $E_2 = E_{\mathbb{Q}}(1,1)$. We commented that this curve is infinite and, getting ahead of ourselves at that stage, we remarked that the group $(E_2, +)$ is isomorphic to the group of integers $\mathbb{Z}$.

Although you do not have the necessary mathematical tools to prove this claim, we can verify how some of the points of $E_{\mathbb{Q}}(1,1)$ listed in Example 2.6 are related in terms of the group operation. Let us begin with the point $P_0 = (x_0, y_0) = (0,1)$. First we determine $2P_0$. As in Worked Exercise 2.15, we apply Lemma 2.10(b) with $a = 1$, $b = 1$, $x_0 = 0$ and $y_0 = 1$, and we obtain $c_0 = \frac{1}{2}$, $d_0 = 1$, $x' = \frac{1}{4}$ and $y' = \frac{9}{8}$, so $\pi'(P_0) = (\frac{1}{4}, \frac{9}{8})$, and by Definition 2.12 we have $2P_0 = -\pi'(P_0) = (\frac{1}{4}, -\frac{9}{8})$.

Next, let us determine the sum of P_1 and P_2 for $P_1 = P_0 = (0,1) = (x_1, y_1)$ and $P_2 = 2P_0 = (\frac{1}{4}, -\frac{9}{8}) = (x_2, y_2)$. Lemma 2.10(a) gives $c = -\frac{17}{2}$, $d = 1$, $x_3 = 72$ and $y_3 = -611$, which implies that $\pi(P_1, P_2) = (72, -611)$. Definition 2.12 applied to $P_1 + P_2$ now tells us that $3P_0 = P_1 + P_2 = -\pi(P_1, P_2) = (72, 611)$.

By more advanced methods it can be shown that the point $P_0 = (0,1)$ is in fact a generator of $(E_2, +)$ and that this group is infinite (and hence isomorphic to $\mathbb{Z}$ by Theorem 2.1 of Book B, Chapter 6). Note also that the inverses of the elements calculated above, that is, $-P_0 = (0,-1)$, $-2P_0 = (\frac{1}{4}, \frac{9}{8})$ and $-3P_0 = (72, -611)$, are also in $(E_2, +)$, which agrees with the list of the first few elements of this group given in Example 2.6.

In the following exercises we calculate groups defined by elliptic curves over various small finite fields.

Worked Exercise 2.17 *An elliptic curve over GF_7*

Determine the group $(E_3, +)$, where E_3 is the elliptic curve $E_{GF_7}(0,2)$, corresponding to the equation $y^2 = x^3 + 2$ over GF_7.

Solution

Checking the seven possible values of x in GF_7 reveals that $x^3 + 2$ is a square over GF_7 if, and only if, $x \in \{0, -1, -2, 3\}$, which then gives the following list of elements of E_3:

$$E_3 = \{\mathcal{O}, (0, \pm 3), (-1, \pm 1), (-2, \pm 1), (3, \pm 1)\}.$$

We see that $|E_3| = 9$, and so by Theorem 3.2 of Book B, Chapter 7 there are only two candidates for the abelian group $(E_3, +)$, namely $\mathbb{Z}_9$ and $\mathbb{Z}_3 \times \mathbb{Z}_3$.

Take $P_0 = (0, 3)$. For the values $a = 0$, $b = 2$, $x_0 = 0$ and $y_0 = 3$, Lemma 2.10(b) returns $c_0 = 0$, $d_0 = \frac{4}{-1} = 3$, $x_0' = 0$ and $y' = 3$, hence $\pi'(P_0) = P_0$ and, by Definition 2.12, $2P_0 = -\pi'(P_0) = -P_0$. The last equality implies that $3P_0 = \mathcal{O}$, that is, the point $P_0 = (0, 3)$ has order 3 in the group $(E_3, +)$. By the same token, the point $-P_0 = (0, -3)$ has also order 3.

Now consider a different point P_0, say, $P_0 = (-1, 1)$. Lemma 2.10(b) applied to $a = 0$, $b = 2$, $x_0 = -1$ and $y_0 = 1$ gives $c_0 = \frac{3}{2} = -2$, $d_0 = \frac{5}{2} = -1$, $x' = -1$ and $y' = 1$. This gives $\pi'(P_0) = P_0$ again, which implies that $2P_0 = -P_0$ again. We have thus discovered another two points of order 3, namely, $(-1, 1)$ and its inverse, $(-1, -1)$.

Since the group $\mathbb{Z}_9$ contains just two elements of order 3, we conclude that the group $(E_3, +)$ is isomorphic to $\mathbb{Z}_3 \times \mathbb{Z}_3$.

As an aside, and addressing the remark immediately following the proof of Lemma 2.10, here we have met the case $\pi'(P_0) = P_0$. In fact, since every non-identity element in $(E_3, +)$ has order 3, it follows that $\pi'(P_0) = P_0$ for every non-identity element of E_3.

Exercise 2.4

Let $E_4 = E_{GF_5}(1, 1)$ be the elliptic curve given by the equation $y^2 = x^3 + x + 1$ over the field GF_5. Determine the group $(E_4, +)$.

Worked Exercise 2.18 *An elliptic curve over GF_{19}*

Determine the group $(E_5, +)$ for the elliptic curve $E_5 = E_{GF_{19}}(1, 4)$ over the field of order 19, corresponding to the equation $y^2 = x^3 + x + 4$ over GF_{19}.

Solution

In examples that involve a slightly larger group, like this one, it is of advantage to be organised. Since we will need to take square roots in $GF_{19} = \{0, \pm 1, \ldots, \pm 9\}$, we start by determining the set of non-zero squares in this field. This can be done in two ways:

- we find a primitive element of GF_{19} – then its even powers are the squares of GF_{19} – or
- we calculate the values of $j^2 \pmod{19}$ for $j \in \{1, \ldots, 9\}$; this range is sufficient since $j^2 = (-j)^2$.

By inspection, one finds that, for example, 2 is a primitive element of GF_{19}, so that the non-zero squares are 2^2, 2^4, ...

For the second approach, a table such as Table 2.3 below is useful.

Table 2.3 The non-zero squares of GF_{19}

j	1	2	3	4	5	6	7	8	9
$j^2 \pmod{19}$	1	4	9	−3	6	−2	−8	7	5

We then arrange the values of $f(x) = x^3 + x + 4$ for $x \in \{0, 1, \ldots, 9\}$ in another table, and in the cases when $f(x)$ is a square (which we may check quickly using Table 2.3) we also give the value of $y = \pm\sqrt{f(x)}$.

Table 2.4 The values of $f(x)$, $x \in \{0, 1, \ldots, 9\}$, with square roots

x	0	1	2	3	4	5	6	7	8	9
x^3	0	1	8	8	7	−8	7	1	−1	7
$f(x)$	4	6	−5	−4	−4	1	−2	−7	−8	1
y	±2	±5	×	×	×	±1	±6	×	±7	±1

The remaining values for $x \in \{-1, -2, \ldots, -9\}$ can be obtained from Table 2.4 by observing that $f(-x) = -f(x) + 8$, so that we may omit the row corresponding to x^3.

Table 2.5 The values of $f(x)$, $x \in \{-1, \ldots, -9\}$, with square roots

x	−1	−2	−3	−4	−5	−6	−7	−8	−9
$f(x)$	2	−6	−7	−7	7	−9	−4	−3	7
y	×	×	×	×	±8	×	×	±4	±8

A list of all pairs $(x, y) \in E_5 \backslash \{\mathcal{O}\}$ now follows from Tables 2.4 and 2.5:

Table 2.6 A list of all the elements of $E_5 \backslash \{\mathcal{O}\}$

x	0	1	5	−5	6	8	−8	9	−9
y	±2	±5	±1	±8	±6	±7	±4	±1	±8

It follows that $|E_5| = 19$. This is very fortunate, as it simplifies our task to determine $(E_5, +)$: since 19 is a prime and the only group of order 19 is the cyclic group $\mathbb{Z}_{19}$ (by Proposition 3.1 of Book B, Chapter 7), it follows that $(E_5, +) \simeq \mathbb{Z}_{19}$. In particular, any of the 18 points (x, y) listed in Table 2.6 is a generator of the group $(E_5, +)$.

Exercise 2.5

Determine the group $(E_6, +)$ for the elliptic curve $E_6 = E_{GF_{13}}(0, 2)$ over the field of order 13, corresponding to the equation $y^2 = x^3 + 2$ over GF_{13}.

Hint: you met this curve in Exercise 2.3.

Exercise 2.6

Determine the group $(E_7, +)$ for the elliptic curve $E_7 = E_{GF_{17}}(1, -1)$ over the field of order 17, corresponding to the equation $y^2 = x^3 + x - 1$ over GF_{17}.

Two substantial results on elliptic curves

The examples in this subsection suggest that determining the abelian group arising from an elliptic curve over the field of rational numbers or over a finite field is a hard problem. This is indeed the case. In what follows, we state just two main results in this direction, accompanied by a few comments.

The main result on groups arising from rational elliptic curves was a joint effort by L. Mordell (1922), A. Weil (1928) and B. Mazur (1977). In the statement of the result below, for any non-negative integer r the symbol $\mathbb{Z}^r$ denotes the trivial group if $r = 0$, and the direct product

$$\underbrace{\mathbb{Z} \times \cdots \times \mathbb{Z}}_{r \text{ times}} \quad \text{if} \quad r \geq 1.$$

Theorem 2.19

Let E be an elliptic curve over the field of rational numbers. Then the group $(E, +)$ is isomorphic to a group of the form $A \times \mathbb{Z}^r$ for some $r \geq 0$, where A is a finite abelian group isomorphic to $\mathbb{Z}_n$ for some $n \in \{1, 2, \ldots, 9, 10, 12\}$, or to $\mathbb{Z}_2 \times \mathbb{Z}_{2m}$ for some $m \in \{1, 2, 3, 4\}$.

It is interesting to note that the relationship of the parameter r, called the *rank* of E, to elliptic curves arising from the rational curve E by 'reduction modulo p' for all sufficiently large prime numbers p, is the subject of the famous *Birch and Swinnerton–Dyer Conjecture*. The conjecture, too advanced to be formulated here, is one of the seven Millennium Problems listed by the Clay Mathematics Institute in 2000, each carrying a prize of 1 000 000 USD for the first correct proof.

A sharp bound on the order of the abelian groups arising from elliptic curves over finite fields was proved by H. Hasse (1933). We will state the bound in combination with a classical result about the structure of these groups.

Theorem 2.20

Let E be an elliptic curve over a finite field of order q. Then the group $(E, +)$ is either cyclic, or isomorphic to a product $\mathbb{Z}_k \times \mathbb{Z}_m$ for some $k, m \geq 2$ such that k is a divisor of m. In either case, the order e_q of the group $(E, +)$ satisfies the inequality

$$|e_q - (q+1)| \leq 2\sqrt{q}.$$

You may want to check that the orders of the groups determined in Example 2.7, Exercise 2.4 and Worked Exercises 2.17 and 2.18 satisfy the structure statement and the inequality in Theorem 2.20.

2.5 Two cryptosystems based on elliptic curves

We begin with the same motivational example as in our discussion of the cryptosystems based on modular arithmetic: imagine that Alice wants to send a message to Bob in such a way that Eve, the eavesdropper, has no realistic chance to know the message, even though Eve knows all the details of the encryption process (except, of course, the message itself). This time, however, we want to employ elliptic curves to do the job.

Among a variety of existing cryptosystems based on elliptic curves, we will present two: the Diffie–Hellman–ElGamal and the Menezes–Vanstone systems. Later in this subsection we will briefly discuss the security of these two systems and some related computational issues.

The Diffie–Hellman–ElGamal elliptic curve cryptosystem

The Diffie–Hellman–ElGamal elliptic curve cryptosystem is based on the 'shared secret' idea of the Diffie–Hellman cryptosystem which you encountered in Subsection 1.5, combined with ElGamal encryption and decryption on an elliptic curve over a finite field. Suppose, as usual, that Alice and Bob want to communicate securely through an insecure channel. In order to set up the communication, Alice and Bob choose an elliptic curve over a finite field together with some parameters, rather like in the setup of a Diffie–Hellman exchange scheme.

Communication setup

Alice and Bob agree a prime p and two elements $a, b \in GF_p$ such that $4a^3 + 27b^2 \neq 0$, so that the selected parameters define an elliptic curve $E = E_{GF_p}(a, b)$. Recall that for a fast generation of large primes with high probability they can use the Rabin–Miller test described in Subsection 1.4. They also agree an initial point $P \in E$; a quick way of generating such a point will be discussed later.

Alice then chooses a positive integer s_A such that $1 < s_A < |E| - 1$. At the other end of the communication line, Bob also chooses a positive integer s_B such that $1 < s_B < |E| - 1$. The integers s_A and s_B are kept secret. Alice then calculates the point $P_A = s_A P \in E$, that is, modulo p, and sends P_A over the channel to Bob. Symmetrically, Bob calculates the point $P_B = s_B P \in E$ and sends P_B to Alice. In this way, both P_A and P_B have been made public.

As part of the setup, Alice also computes the point $s_A P_B$ in E using her private key s_A, and Bob computes the point $s_B P_A$ with the help of his private key s_B. Since $s_A P_B = s_A(s_B P) = s_B(s_A P) = s_B P_A$, Alice and Bob obtain the same point. We will denote this resulting point by Q; this will not be released and will remain a shared secret between Alice and Bob. The shared secret Q will not play any role in what follows, but is important in practice; we will briefly touch upon this issue at the end of this chapter.

To sum up, the quadruple (E, P, P_A, P_B) is the public key in this system, and the integers s_A and s_B are respectively Alice's and Bob's private keys.

Encryption

Suppose Alice wants to send Bob a message. First she must convert her message into a point on the elliptic curve E; a way to do this will be introduced later. For now, assume that the message Alice wants to send has been encoded in the form of a point M on E. She generates a random positive integer k, $1 < k < |E|$, and she uses the public key (E, P, P_A, P_B) to compute two points in the group $(E, +)$: the point $M_1 = kP$ and the point $M_2 = M + kP_B$. Note that only M_2 depends on the message M; both M_1 and M_2, however, depend on the integer k known only to Alice. She then sends M_1 and M_2 to Bob through the communication channel, so that anybody, including Eve, can get hold of M_1 and M_2.

Decryption

After receiving M_1 and M_2, Bob performs an amazingly simple calculation: using his private key, s_B, he computes the point $M_2 - s_B M_1$ in the group $(E, +)$. But even without knowledge of k, the way M_1 and M_2 have been created and the fact that $P_B = s_B P$ give

$$M_2 - s_B M_1 = (M + kP_B) - s_B(kP) = M + k(s_B P) - s_B(kP) = M$$

and hence $M_2 - s_B M_1$ is equal to the original message M (as a point on the curve E).

Comments

In this setting, communication can go both ways, as in the Diffie–Hellman system. If Bob wants to send Alice a message $M' \in E$, he generates a random integer k', $1 < k' < |E|$, and computes $M'_1 = k'P$ and $M'_2 = M' + k'P_A$. After receiving M'_1 and M'_2, Alice decrypts Bob's message by computing $M'_2 - s_A M'_1$, which is equal to M' by an analogous computation as above.

A deeper analysis, details of which are beyond the scope of this module, shows that if Eve had a general method to decipher Alice's message M and Bob's message M', then she would be able to determine their secret keys, too. To make this cryptosystem as secure as possible, one has to make sure that attempts to determine s_A and s_B from the knowledge of the points P, $P_A = s_A P$ and $P_B = s_B P$ are hopeless. We will discuss the security of this cryptosystem later in this chapter. For now we just note what you would expect – namely, the prime p we have begun with should be large to make breaking attempts infeasible.

In our description, we have assumed that Alice's message is a point of an elliptic curve $E = E_{GF_p}(a, b)$. In other words, we have assumed that M is of the form $M = (x, y)$, where x and y are elements of GF_p that satisfy the equation $y^2 = x^3 + ax + b$ modulo p. Now, if p is extremely large, how can Alice and Bob find solutions of this equation at all? And, assuming they have a procedure for finding the solutions, how can they convert a plain text message into a point on the curve?

Before addressing these questions, we give a concrete example of encryption and decryption with the help of an elliptic curve.

Example 2.21 *The Diffie–Hellman–ElGamal system: encryption and decryption*

Suppose that Alice and Bob have chosen $p = 19$, $a = 1$ and $b = 4$. This means that their elliptic curve is $E = E_{GF_{19}}(1, 4)$, corresponding to the equation $y^2 = x^3 + x + 4$ (in GF_{19}, that is, modulo 19). Note that we worked with this curve in Worked Exercise 2.18. Suppose further that they have agreed to use the point $P = (0, 2) \in E$.

Bob decides to have $s_B = 4$ as his private key and needs to compute the point $P_B = s_B P$. You may check that an evaluation using Definition 2.12(d) and Lemma 2.10(b) gives $2P = (6, 6)$ and $4P = 2(2P) = (-8, 4)$. It follows that Bob's point is $P_B = (-8, 4)$, which he sends through the channel.

Suppose Alice wants to send Bob the message $M = (1, 5) \in E$. According to the procedure outlined above, Alice randomly chooses a positive integer, say $k = 3$ for the sake of this example. She now needs to determine $M_1 = 3P$ and $M_2 = M + 3P_B$. To determine $3P$ she first determines $2P$ and then $3P = P + 2P$. Since we know that $2P = (6, 6)$, Definition 2.12(e) and Lemma 2.10(a) imply that $M_1 = 3P = P + 2P = (5, 1)$. Similarly, from $P_B = (-8, 4)$ she obtains $2P_B = (1, -5)$ and $3P_B = P_B + 2P_B = (8, -7)$. Finally, Alice computes $M_2 = M + 3P_B = (-8, 4)$ and sends $M_1 = (5, 1)$ and $M_2 = (-8, 4)$ to Bob through the communication channel.

After receiving M_1 and M_2, Bob calculates $s_B M_1 = 4M_1$; we omit the details of Bob's calculations and just note that he obtains $4M_1 = (8, -7)$. He can then recover the message by calculating $M_2 - 4M_1$; we look at this last calculation in somewhat more detail. We have

$$M_2 + (-4M_1) = (-8, 4) + (8, 7).$$

Lemma 2.10(a) applied to the values $a = 1$, $b = 4$, $(x_1, y_1) = (-8, 4)$ and $(x_2, y_2) = (8, 7)$ gives, modulo 19,

$$c = \frac{7-4}{8-(-8)} = \frac{3}{-3} = -1,$$
$$d = \frac{32+56}{-3} = \frac{-7}{-3} = -4,$$
$$x_3 = 1 - 8 + 8 = 1, \quad \text{and finally}$$
$$y_3 = -1 - 4 = -5.$$

By Definition 2.12(e), we conclude that $M_2 - 4M_1 = (1, 5)$, which is indeed the original message.

Exercise 2.7

Alice and Bob agree to use the Diffie–Hellman–ElGamal system with the elliptic curve $E = E_{GF_{17}}(1, -1)$ from Exercise 2.6. They use the public key (E, P, P_A, P_B), where $P = (0, 4)$, $P_A = (4, 4)$, $P_B = (-4, -4)$. Alice's and Bob's private keys are $s_A = 2$ and $s_B = 3$ respectively. Alice wants to send Bob the message $M = (8, -3)$ using the randomly generated integer $k = 5$. Determine Alice's ciphertext and verify its correct decryption by Bob.

The Menezes–Vanstone elliptic curve cryptosystem

If Alice and Bob were to use the Diffie–Hellman–ElGamal system to exchange a large number of messages, they would have to have a quick means to generate points on an elliptic curve to encode their messages. While, as we shall see later, this is not an obstacle in reality, there is a way to bypass this requirement and encrypt messages in a slightly different form that avoids repeated generation of points on an elliptic curve. The method was proposed by Menezes and Vanstone in 1993.

Communication setup

This step is identical to the setup of Diffie–Hellman–ElGamal cryptosystem: the public key is a quadruple (E, P, P_A, P_B), and Alice's and Bob's private key are s_A and s_B respectively, as before.

Encryption

Alice's message now has the form of an ordered pair (m_1, m_2), where $m_1, m_2 \in \mathbb{Z}_p$ and p is the order of the field GF_p over which Alice's and Bob's elliptic curve is defined. So now Alice does not need to generate points on E. Instead, she chooses a random positive k such that $1 < k < |E|$. Knowing P and P_B allows her to compute the points $kP \in E$ and $kP_B \in E$. Let the coordinates of the second point be $kP_B = (d_1, d_2)$. Alice finally computes $c_1 = d_1 m_1 \in \mathbb{Z}_p$ and $c_2 = d_2 m_2 \in \mathbb{Z}_p$. Her ciphertext is the triple (kP, c_1, c_2), which she sends to Bob through the communication channel.

Decryption

To decrypt this ciphertext, Bob first determines the pair (d_1, d_2) by multiplying the point kP in Alice's message by his private key s_B, since

$$s_B(kP) = k(s_BP) = kP_B = (d_1, d_2).$$

Using the Euclidean Algorithm as in the solution to Worked Exercise 1.2, he then determines d_1^{-1} and d_2^{-1} modulo p. Finally, Bob recovers Alice's message (m_1, m_2) by multiplying the second and third components of her ciphertext, c_1 and c_2, by d_1^{-1} and d_2^{-1} modulo p. Indeed, $m_1 = c_1 d_1^{-1}$ and $m_2 = c_2 d_2^{-1}$, all modulo p.

Comments

The symmetry of this scheme allows Alice and Bob to communicate both ways. This scheme greatly enlarges the number of messages Alice can send, as her messages are now ordered pairs of elements of $\mathbb{Z}_p$, rather than points on an elliptic curve over GF_p. The number of such ordered pairs is p^2, which is much larger than the number of points on an elliptic curve over GF_p, which is approximately p by Hasse's Theorem (Theorem 2.20).

Example 2.22 *The Menezes–Vanstone system: encryption and decryption*

We will again work with the elliptic curve $E = E_{GF_{19}}(1, 4)$, corresponding to the equation $y^2 = x^3 + x + 4$ in GF_{19}, as in Example 2.21. To simplify matters, let us assume that Alice and Bob agree to use the same base point $P = (0, 2)$ as in Example 2.21. Suppose further that Alice and Bob choose the values $s_A = 4$ and $s_B = 3$ as their private keys, respectively.

We will now use the results of our computations in Example 2.21. Alice computes $s_AP = 4P = (-8, 4)$, Bob determines $s_BP = 3P = (5, 1)$, and they make these results public by sending them to each other through the communication channel.

As in the examples illustrating the public-key cryptosystems in Section 1, suppose that Alice wants to send Bob the three-digit security number, 609, on yet another credit card. Assume that Alice and Bob have agreed to form a four-digit number out of the security number by inserting a zero in the front, so that Alice's message is $(m_1, m_2) = (06, 09)$.

Suppose that Alice has chosen $k = 5$. With the help of Definition 2.12 and Lemma 2.10, she computes $kP = 5P = (-5, -8)$ and $k(P_B) = 5(5, 1) = (-8, -4)$. Thus, Alice finds that $d_1 = -8$ and $d_2 = -4$. This enables her to compute

$$c_1 = d_1 m_1 = -48 \equiv 9 \pmod{19} \quad \text{and}$$
$$c_2 = d_2 m_2 = -36 \equiv 2 \pmod{19}.$$

Alice then sends the ciphertext $(kP, c_1, c_2) = ((-5, -8), 9, 2)$ through an insecure channel to Bob.

To decrypt the ciphertext, Bob computes $s_B(kP) = 3(-5,-8) = (-8,-4)$, so that $d_1 = -8$ and $d_2 = -4$. Inverting d_1 and d_2 he obtains $d_1^{-1} = 7$ and $d_2^{-1} = -5$. He finally recovers

$$m_1 = c_1 d_1^{-1} = \quad 63 \equiv 6 \pmod{19} \quad \text{and}$$
$$m_2 = c_2 d_2^{-1} = -10 \equiv 9 \pmod{19}.$$

Bob can now concatenate $m_1 = 06$ and $m_2 = 09$, and by deleting the leftmost zero he obtains Alice's security number, 609.

Exercise 2.8

Alice and Bob choose to use the Menezes–Vanstone cryptosystem with the elliptic curve $E = E_{GF_{17}}(1,-1)$ from Exercise 2.7. They use again the public key (E, P, P_A, P_B), where

$$P = (0,4),\ P_A = (4,4),\ P_B = (-4,-4),$$

and their private keys are $s_A = 2$ and $s_B = 3$ respectively. Alice wants to send Bob the message $(m_1, m_2) = (2,4)$ using the randomly generated integer $k = 4$. Determine Alice's ciphertext and verify its correct decryption by Bob.

Security of cryptosystems based on elliptic curves

In general, it would seem that the only feasible way to break the cryptosystems based on elliptic curves that we have just described is to determine Alice's and Bob's private keys, s_A and s_B, from the equations $P_A = s_A P$ and $P_B = s_B P$, where the three points P, P_A and P_B lying on an elliptic curve are public knowledge. This is a special case of a more general problem, the *discrete logarithm problem for elliptic curves*. The discrete logarithm for elliptic curves is defined next.

Definition 2.23 *Discrete logarithm for elliptic curves*

Let $E = E_{GF_p}(a,b)$ be an elliptic curve over a Galois field GF_p. Let $P, P' \neq \mathcal{O}$ be two points on E, regarded as elements of the abelian group $(E,+)$. If there exists an integer s, $1 < s < |E|$, such that $P' = sP$, then s is called the **discrete logarithm of P' to the base P**.

Observe the analogy with Definition 1.15 of the discrete logarithm for finite fields. The difference is that in the context of elliptic curves the exponentiation operation is replaced by multiplication. Moreover, here, if $(E,+)$ is a cyclic group and P is a generator of this group, then the discrete logarithm to the base P exists for any point $P \in E$.

It turns out that there are no known efficient algorithms to solve the discrete logarithm problem for elliptic curves, that is, to work out the

discrete logarithm of an elliptic curve to a given base. The best known algorithms to break a cryptosystem based on an elliptic curve defined over a field GF_p need about $c \times \sqrt{p}$ operations, where c is a constant. This vastly exceeds, for example, the number of operations needed to factorise a number of a similar size by the general number sieve algorithm. So in the case of elliptic curves we are in a better position, since elliptic curve cryptosystems defined over GF_p appear to be safe when p is a prime number about 250 bits long. In fact, elliptic curve cryptosystems appear to prevail and outperform other systems.

Fast generation of points on an elliptic curve

The last question to be addressed for elliptic curve cryptosystems is how one can generate points on an elliptic curve quickly, that is, in real time.

Let $E = E_{GF_p}(a, b)$ be an elliptic curve over the finite field GF_p, where p is a large odd prime. We know that $E\backslash\{\mathcal{O}\}$ is the set of all ordered pairs (x, y) such that $y^2 = x^3 + ax + b$. The task is to generate a point $P = (x, y)$ on E, that is, to find a solution (x, y) of the equation $y^2 = x^3 + ax + b$. By Hasse's Theorem we know that there are at least $p - 2\sqrt{p}$ such points, but the theorem does not tell us how to find them. We would like to emphasise that points of the form $P = (x, 0)$ are not of much use, since by Definition 2.12 doubling gives $2P = \mathcal{O}$.

There is an astonishingly simple method for generating such points quickly. As in the case of generating prime numbers in Subsection 1.4, it is based on probabilistic considerations. Certain results in probability theory tell us that if x is a random non-zero element of GF_p, the element $x^3 + ax + b$ may also be considered to be random (and non-zero, by the above remark). For such an x to generate a point (x, y) on E, the (random) element $x^3 + ax + b$ would have to have a square root y. This is the same as saying that $x^3 + ax + b$ would have to be a square, or, in the terminology of Definition 1.2 of Book C, Chapter 10, a quadratic residue. Now, what are the chances that a random element of GF_p is a square? Since for an odd P the field GF_p contains the same number of non-zero squares and non-squares, that is, $(p - 1)/2$, the probability of a randomly chosen element in GF_p to be a square is $\frac{1}{2}$.

This suggests that points on E can be found as follows. Suppose for simplicity that $p \equiv -1 \pmod 4$ and let $f(x) = x^3 + ax + b$. Take a random $x \in GF_p$ and successively test the values $f(x)$, $f(x + 1)$, $\ldots$, $f(x + j)$ by Euler's Criterion for quadratic residues (Subsection 1.1, Lemma 1.9). As indicated above, the probability that none of these are a quadratic residue modulo p is about 2^{-j}, which gets extremely small as j gets larger. So, with high probability, within a few steps this method generates an x such that $f(x)$ is a square modulo p. If, in addition, $p \equiv -1 \pmod 4$, one can quickly determine the solutions $\pm y$ of $y^2 = f(x)$ using the second part of Lemma 1.9.

This procedure can also be adapted to encode plaintext messages in the form of points on E. Indeed, as we know, any plaintext messages can be identified with a decimal number; we assume that the number is a positive integer z such that $z < \frac{|E|}{1000}$, say. Now, among the numbers $f(100z)$, $f(100z+1)$, $\ldots$, $f(100z+99)$ with high probability there will be one, say $f(100z+j)$ for some $j \in \{0,1,\ldots,99\}$, such that $f(100z+j)$ is a square in GF_p. Let $x = 100z + j$. Then the point $M = (x, y)$ with $y^2 = f(x)$ can then be taken to be the point on E encoding the message M. The person decrypting the message then simply discards the last two decimal digits of x to obtain z.

We reiterate that all these computations can be done extremely quickly by the squaring method introduced in Subsection 1.1.

A note on practical aspects

The ideas explained in this chapter have been automated and integrated into communication systems.

In a very simplified model, suppose that Alice and Bob want to communicate securely over the internet. When, say, Alice sends a request to Bob, her browser and Bob's browser first 'shake hands' and select a cryptosystem to be used for their communication. The selection is made from a rather narrow predefined set of cryptosystems that meet high international standards.

The most recommended model of secure communication appears to be a Diffie–Hellman key exchange combined with other techniques that require the shared secret as a seed for further encryption. The details, however, are way too complex to be included in this brief overview of algebraic methods used in public-key cryptography.

Learning outcomes

We list those topics on which we may set assessment questions to test your understanding of the chapter.

After working through this chapter you should be able to:

(a) Find the highest common factor of two appropriate integers using the Fast Euclidean Algorithm.

(b) Where appropriate find the multiplicative inverse of one integer modulo another by reversing the Fast Euclidean Algorithm.

(c) Where appropriate find a witness of non-primality.

(d) Find a primitive element of GF_p provided p is not too large.

(e) Check whether integers are quadratic residues mod p and find square roots in GF_p provided p is not too large.

(f) Use the RSA cryptosystem for suitable primes.

(g) Use the Diffie–Hellman cryptosystem for a suitable prime.

(h) Identify points on an elliptic curve in appropriate cases.

(i) Draw an elliptic curve in simple cases.

(j) Compute $\pi(P_1, P_2)$ and $\pi\prime(P_0)$ for given points P_0, P_1, P_2 on an elliptic curve.

(k) Identify the group $(E, +)$ for an elliptic curve in very simple cases.

(l) Use the Diffie–Hellman–ElGamal cryptosystem in simple cases.

(m) Use the Menezes–Vanstone cryptosystem in simple cases.

Solutions to exercises

Solution to Exercise 1.1

Suppose that $\text{hcf}(r, s) = h$. Then h is a common factor of r and $r - s$ by Theorem 4.4(e) of Book A, Chapter 1.

Now let k be a common factor of r and $r - s$. Then $km = r$ and $kn = r - s$ for some integers m and n. But then

$$kn = r - s = km - s,$$

which implies that $s = k(m - n)$. Hence k is a common factor of r and s. It follows that k divides h, so h is the highest common factor of r and $r - s$.

Solution to Exercise 1.2

Since $19\,191 < \frac{91\,919}{2}$, the input for step S_0 in the Fast Euclidean Algorithm is the pair $(91\,919, 19\,191)$. In the notation of the solution to Worked Exercise 1.1, we obtain the following steps.

$$\begin{array}{lrcll}
S_0: & 91\,919 & = & 4 \times \underline{19\,191} + \underline{\underline{15\,155}} & \text{use } \underline{4036} = 19\,191 - 15\,155 \text{ in } S_1 \\
S_1: & 19\,191 & = & 4 \times \underline{4036} + \underline{\underline{3047}} & \text{use } \underline{989} = 4036 - 3047 \text{ in } S_2 \\
S_2: & 4036 & = & 4 \times \underline{989} + \underline{\underline{80}} & \text{use } \underline{80} \text{ in } S_3 \\
S_3: & 989 & = & 12 \times \underline{80} + \underline{\underline{29}} & \text{use } \underline{29} \text{ in } S_4 \\
S_4: & 80 & = & 2 \times \underline{29} + \underline{\underline{22}} & \text{use } \underline{7} = 29 - 22 \text{ in } S_5 \\
S_5: & 29 & = & 4 \times \underline{7} + \underline{\underline{1}} &
\end{array}$$

Therefore $\text{hcf}(91\,919, 19\,191) = 1$.

Solution to Exercise 1.3

The multiplicative inverse of 19 191 modulo 91 919 exists by Exercise 1.2. Taking the equation in step S_5 of this exercise, working backwards and taking into account the replacements in the Fast Euclidean Algorithm (as in the solution to Worked Exercise 1.2) gives

$$\begin{aligned}
1 &= 29 - 7 \times 4 = 29 - \underline{(29 - 22)} \times 4 \\
&= 29 \times (-3) + 22 \times 4 \\
&= 29 \times (-3) + (80 - 2 \times 29) \times 4 \\
&= 80 \times 4 - 29 \times 11 \\
&= 80 \times 4 - (989 - 12 \times 80) \times 11 \\
&= 989 \times (-11) + 80 \times 136 \\
&= 989 \times (-11) + (4036 - 4 \times 989) \times 136 \\
&= 4036 \times 136 - 989 \times 555 = 4036 \times 136 - \underline{(4036 - 3047)} \times 555 \\
&= 4036 \times (-419) + 3047 \times 555 \\
&= 4036 \times (-419) + (19\,191 - 4 \times 4036) \times 555 \\
&= 19\,191 \times 555 - 4036 \times 2639 = 19\,191 \times 555 - \underline{(19\,191 - 15\,155)} \times 2639 \\
&= 19\,191 \times (-2084) + 15\,155 \times 2639 \\
&= 19\,191 \times (-2084) + (91\,919 - 4 \times 19\,191) \times 2639 \\
&= 91\,919 \times 2639 - 19\,191 \times 12\,640.
\end{aligned}$$

The multiplicative inverse of 19 191 modulo 91 919 is $-12\,640$, which modulo 91 919 is the same as $91\,919 - 12\,640 = 79\,279$.

Solution to Exercise 1.4

Observe that $899 = 29 \times 31$, $840 = (29-1) \times (31-1)$ and $841 = 29^2$. Let $n = 899, p = 29$, $q = 31$ and $d = e = 29$. Then $n = pq = 899$, $\phi(n) = 840$ and $de \equiv 1 \pmod{\phi(n)}$. By Lemma 1.3 we have $x^{841} \equiv x \pmod{899}$ for all integers x.

Solution to Exercise 1.5

We test the simplest b, that is, $b = 2$. Since $k - 1 = 288 = 2^5 \times 9$, we have $r = 5$ and $s = 9$. We evaluate the following congruences modulo 289 by repeatedly raising the left-hand side to the power 2.

$$\begin{aligned} 2^{9} &\equiv -66 \\ 2^{2\times 9} &\equiv 21 \\ 2^{2^2\times 9} &\equiv -137 \\ 2^{2^3\times 9} &\equiv -16 \\ 2^{2^4\times 9} &\equiv -33 \end{aligned}$$

By Corollary 1.5 the integer $b = 2$ is a witness of non-primality of $k = 289$ (note that $289 = 17^2$).

Solution to Exercise 1.6

Since $p = 257$ and $p - 1 = 256 = 2^8$, Lemma 1.7 tells us that a non-zero $\xi \in GF_{257}$ is a primitive element if, and only if, $\xi^{2^7} \not\equiv 1 \pmod{257}$. The element $\xi = 2$ will not work since $2^{2^3} \equiv -1 \pmod{257}$ and so $2^{2^7} \equiv 1 \pmod{257}$. Let us try $\xi = 3$. By squaring we find that, modulo 257,

$$\begin{aligned} 3^{2^2} &\equiv 81 \\ 3^{2^3} &\equiv 136 \\ 3^{2^4} &\equiv -8 \\ 3^{2^5} &\equiv 64 \\ 3^{2^6} &\equiv -16 \\ 3^{2^7} &\equiv -1. \end{aligned}$$

We conclude that $\xi = 3$ is a primitive element of GF_{257} by Lemma 1.7.

Solution to Exercise 1.7

Here $p = 193$ and $\frac{p-1}{2} = 96$. We have $(-1)^{96} \equiv 1 \pmod{193}$, and with the help of the calculations in the solution of Worked Exercise 1.8 we obtain $3^{96} = (3^8)^{12} = (-1)^{12} \equiv 1 \pmod{193}$ and $(-5)^{96} = 5^{96} \equiv -1 \pmod{193}$. By Lemma 1.9, we see that -1 and 3 are squares modulo 193 while -5 is not. Note that 5 is a primitive element of GF_{193} and hence it cannot be a square; a product of a square and a non-square is a non-square, which gives another proof that -5 is a non-square.

As $193 \equiv 1 \pmod{4}$, we cannot use the second part of Lemma 1.9 to determine the square roots of -1 and 3. With relatively small moduli, experiments with squares of integers usually help. Since $14^2 = 196 \equiv 3 \pmod{193}$, the square roots of $3 \pmod{193}$ are ± 14. Further, observe that $31^2 \equiv -4 \pmod{193}$; multiplying this congruence by 2^{-1} gives $(31 \times 2^{-1})^2 \equiv -1 \pmod{193}$. The multiplicative inverse 2^{-1} of 2 modulo 193 is $2^{-1} = 97$, and since $31 \times 97 \equiv 112 \pmod{193}$ we conclude that the square roots of -1 modulo 193 are ± 112.

Solution to Exercise 1.8

(a) Using the method and notation in the solution to Example 1.12, Alice obtains the following congruences modulo 5963.

$$
\begin{aligned}
&m_0 = 1111,\\
&m_0^2 = 1\,234\,321, \quad && m_1 \equiv m_0^2 \equiv m^{2^1} \equiv 5943\\
&m_1^2 = 35\,319\,249, && m_2 \equiv m_1^2 \equiv m^{2^2} \equiv 400\\
&m_2^2 = 160\,000, && m_3 \equiv m_2^2 \equiv m^{2^3} \equiv 4962\\
&m_3^2 = 24\,621\,444, && m_4 \equiv m_3^2 \equiv m^{2^4} \equiv 217\\
&m_4^2 = 47\,089, && m_5 \equiv m_4^2 \equiv m^{2^5} \equiv 5348\\
&m_5^2 = 28\,601\,104, && m_6 \equiv m_5^2 \equiv m^{2^6} \equiv 2556\\
&m_6^2 = 6\,533\,136, && m_7 \equiv m_6^2 \equiv m^{2^7} \equiv 3651
\end{aligned}
$$

Alice can then determine the product $m^{203} \equiv m_7 m_6 m_3 m_1 m_0 \pmod{5963}$:

$m_7 m_6 \equiv 5824 \pmod{5963}$

$m_7 m_6 m_3 \equiv 5824 m_3 \equiv 1990 \pmod{5963}$

$m_7 m_6 m_3 m_1 \equiv 1990 m_1 \equiv 1941 \pmod{5963}$.

Finally, she obtains her ciphertext:

$$c \equiv m_7 m_6 m_3 m_1 m_0 \equiv 1941 m_0 = 2\,156\,451 \equiv 3808 \pmod{5963}.$$

(b) Bob begins the decryption procedure by writing his private key as a sum of powers of two:

$$d = 515 = 2^9 + 2^1 + 2^0.$$

Letting $c_0 = c$, he successively computes $c_1 \equiv c^{2^1} \pmod{n}$, $c_2 \equiv c_1^2 = c^{2^2} \pmod{n}$, $c_3 \equiv c_2^2 = c^{2^3} \pmod{n}$, and so on, up to $c_9 \equiv c_8^2 = c^{2^9} \pmod{n}$, and using these he finally determines

$$c^{515} = c^{2^9 + 2^1 + 2^0} \equiv c_9 c_1 c_0 \pmod{n}.$$

These individual steps give the following congruences modulo 5963:

$$
\begin{aligned}
&c_0 = 3808,\\
&c_0^2 = 14\,500\,864, \quad && c_1 \equiv c_0^2 \equiv c^{2^1} \equiv 4811\\
&c_1^2 = 23\,145\,721, && c_2 \equiv c_1^2 \equiv c^{2^2} \equiv 3318\\
&c_2^2 = 11\,009\,124, && c_3 \equiv c_2^2 \equiv c^{2^3} \equiv 1426\\
&c_3^2 = 2\,033\,476, && c_4 \equiv c_3^2 \equiv c^{2^4} \equiv 93\\
&c_4^2 = 8649, && c_5 \equiv c_4^2 \equiv c^{2^5} \equiv 2686\\
&c_5^2 = 7\,214\,596, && c_6 \equiv c_5^2 \equiv c^{2^6} \equiv 5329\\
&c_6^2 = 28\,398\,241, && c_7 \equiv c_6^2 \equiv c^{2^7} \equiv 2435\\
&c_7^2 = 5\,929\,225, && c_8 \equiv c_7^2 \equiv c^{2^8} \equiv 2003\\
&c_8^2 = 4\,012\,009, && c_9 \equiv c_8^2 \equiv c^{2^9} \equiv 4873.
\end{aligned}
$$

Bob can now calculate $c^{227} \equiv c_9 c_1 c_0 \pmod{5963}$:

$$c_9 c_1 \equiv 3450.$$

The final result Bob obtains is

$$c^{515} \equiv c_9 c_1 c_0 \equiv 3450 c_0 \equiv 1111,$$

which is indeed Alice's intended message.

For completeness, note that $n = 5963 = pq$, where $p = 67$, $q = 89$, and $\phi(n) = (p-1)(q-1) = 5808$; one may verify that $e = 203$ and $d = 515$ satisfy $de \equiv 1 \bmod \phi(n)$.

Solution to Exercise 1.9

In this solution, calculations are all modulo 193.

Alice needs to determine $\alpha = \xi^a = 5^{12}$ and Bob needs to determine $\beta = \xi^b = 5^{17}$. Noting that $12 = 2^3 + 2^2$ and $17 = 2^4 + 2^0$ and using $5^{2^0} = 5$, $5^{2^1} \equiv 25$, $5^{2^2} \equiv 46$, $5^{2^3} \equiv 186$ and $5^{2^4} \equiv 49$, Alice obtains $\alpha \equiv 186 \times 46 \equiv 64$ and Bob obtains $\beta \equiv 49 \times 5 \equiv 52$.

One may verify that $\beta^a \equiv \alpha^b \equiv 64 \pmod{193}$, giving the value $\sigma = 64$. The multiplicative inverse σ^{-1} can be determined by the Euclidean Algorithm: since $193 = 3 \times 64 + 1$, it follows immediately that $\sigma^{-1} \equiv -3 \equiv 190 \pmod{193}$.

Alice encrypts the message $m = 123$ by evaluating $c = m\sigma = 123 \times 64 \equiv 152 \pmod{193}$.

Bob decrypts the ciphertext by computing $c\sigma^{-1} = 152 \times (-3) \equiv 123 \pmod{193}$.

Solution to Exercise 2.1

We prove the contrapositive, so we assume that $f(x)$ has at least one multiple root. Suppose that x_0 is a root of $f(x)$ of multiplicity at least two and let x_1 be the third root of $f(x)$. Then we have

$$f(x) = (x - x_0)^2(x - x_1) = x^3 - (2x_0 + x_1)x^2 + (x_0^2 + 2x_0x_1)x - x_0^2x_1.$$

But we have also assumed that $f(x) = x^3 + ax + b$. Comparing the coefficients of x^2 gives $2x_0 + x_1 = 0$, that is, $x_1 = -2x_0$. Using this fact and comparing the remaining coefficients gives $a = x_0^2 + 2x_0x_1 = -3x_0^2$ and $b = -x_0^2x_1 = 2x_0^3$. It follows that $4a^3 + 27b^2 = 4(-3x_0^2)^3 + 27(2x_0^3)^2 = 0$.

Note that when $x_0 = x_1$, the polynomial $f(x)$ has a single root of multiplicity 3, and comparing coefficients as above gives $a = b = 4a^3 + 27b^2 = 0$.

Solution to Exercise 2.2

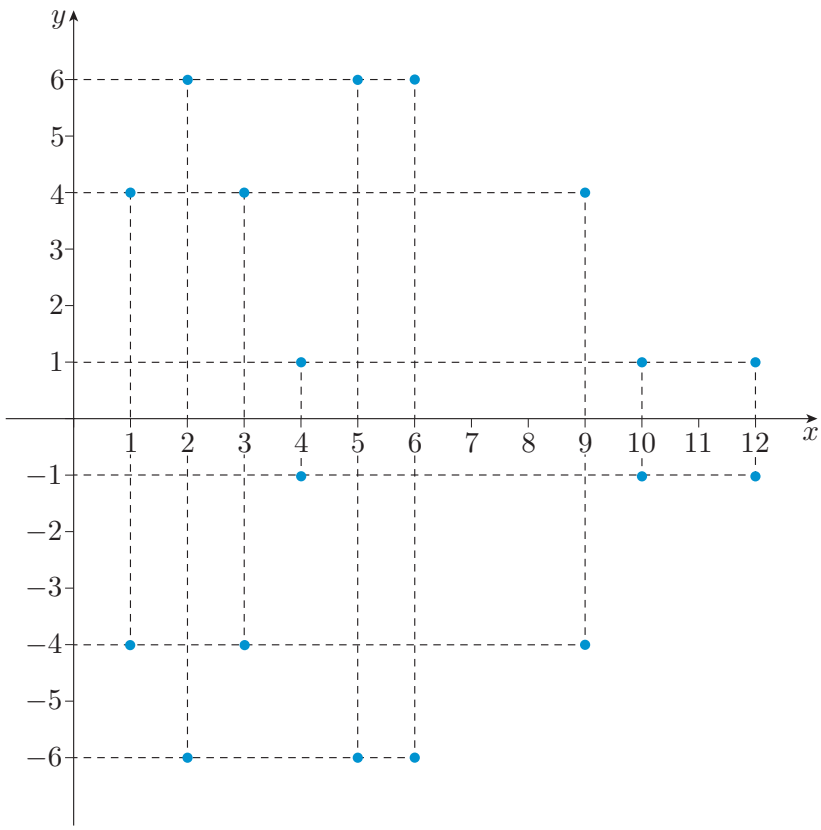
Trying the 11 integer values of x such that $0 \leq x \leq 10$ gives exactly four points on $E_{\mathbb{Q}}(1, 9)$ with integer coordinates $(0, \pm 3)$ and $(8, \pm 23)$.

Solution to Exercise 2.3

We need to identify the set of all $(x, y) \in GF_{13} \times GF_{13}$ such that $y^2 = x^3 + 2$. Since the prime $p = 13$ is not congruent to 2 modulo 3, we cannot use the methods of Example 2.7. However, the field GF_{13} is small enough that for every $x \in GF_{13}$ we can work out $x^3 + 2 \in GF_{13}$.

x	0	1	2	3	4	5	6	7	8	9	10	11	12
$x^3 + 2$	2	3	10	3	1	10	10	7	7	3	1	7	1

By inspection, we find that the set of squares in GF_{13} is $S = \{0, 1, 3, 4, 9, 10, 12\}$. To find the points of $E_{GF_{13}}(0, 2)\backslash\{\mathcal{O}\}$, it suffices to select those $x \in GF_{13}$ such that $x^3 + 2 \in S$, so that the points $(x^3 + 2, \pm\sqrt{x^3 + 2})$ are on the curve. The resulting graph is given below.



A graph of the elliptic curve $E_{GF_{13}}(0,2)\backslash\{\mathcal{O}\}$

Solution to Exercise 2.4

By letting x range over the five possible elements of GF_5, we find that $x^3 + x + 1$ is a square in GF_5 if, and only if, $x \neq 1$. Then

$$E_4 = \{\mathcal{O}, (0, \pm 1), (-1, \pm 2), (2, \pm 1), (-2, \pm 1)\}.$$

We see that $|E_4| = 9$ as in Worked Exercise 2.17, although the underlying fields and the defining polynomials are different. Therefore the candidates for the group $(E_4, +)$ are, again, $\mathbb{Z}_9$ and $\mathbb{Z}_3 \times \mathbb{Z}_3$.

Let us take $P_0 = (0, 1)$ and calculate $2P_0$. Lemma 2.10(b) with $a = b = 1$, $x_0 = 0$ and $y_0 = 1$ gives $c_0 = \frac{1}{2} = -2$, $d_0 = 1$, $x' = 4 = -1$ and $y' = 3 = -2$, so that $2P_0 = -\pi'(P_0) = (-1, 2)$.

Letting $P_1 = P_0 = (0, 1)$ and $P_2 = 2P_0 = (-1, 2)$ and applying Lemma 2.10(a) gives $c = -1$, $d = 1$, $x_3 = 2$ and $y_3 = -1$, so $3P_0 = P_1 + P_2 = -\pi(P_1, P_2) = (2, 1)$.

It follows that the order of the point P_0 in $(E_4, +)$ is different from 3, and therefore the group $(E_4, +)$ must be isomorphic to $\mathbb{Z}_9$. Our calculations also show that P_0 is a generator of this cyclic group.

Solution to Exercise 2.5

We can use the table and the graph of this curve in the solution to Exercise 2.3 or we can follow the method outlined in the solution to Worked Exercise 2.18 to list the points on this curve. We find that

$$E_6 = \{\mathcal{O}\} \cup \{(1, \pm 4), (2, \pm 6), (3, \pm 4), (4, \pm 1), (5, \pm 6), (6, \pm 6), (-4, \pm 4), (-3, \pm 1), (-1, \pm 1)\},$$

and so $|E_6| = 19$. It follows that $(E_6, +) \cong \mathbb{Z}_{19}$. Note that here the underlying field has order 13 only!

Solution to Exercise 2.6

As in the solution to Worked Exercise 2.18, we list the points on the curve. We obtain

$$E_7 = \{\mathcal{O}\} \cup \{(0, \pm 4), (1, \pm 1), (2, \pm 3), (4, \pm 4), (6, 0), (7, \pm 3), (8, \pm 3), (-6, \pm 7), (-4, \pm 4)\},$$

and so $|E_7| = 18$.

By Theorem 2.2 of Book B, Chapter 8, there are just two abelian groups of order 18, namely, $\mathbb{Z}_{18}$ and $\mathbb{Z}_3 \times \mathbb{Z}_6$. To find out which of these is isomorphic to $(E_7, +)$, we experiment with some point, say $P = (0, 4)$. By Lemma 2.10(b), we find that $2P = (4, 4)$ and by part (a) of the same lemma we obtain $3P = (-4, -4)$; a further application of part (b) of the lemma gives $6P = (7, -3)$. Since by Proposition 2.10 of Book B, Chapter 6, the order of every element of $\mathbb{Z}_3 \times \mathbb{Z}_6$ divides 6, it follows that $(E_7, +) \cong \mathbb{Z}_{18}$.

More information is revealed if one uses Lemma 2.10(a) to determine $9P = 6P + 3P = (6, 0)$. The point $(6, 0)$ has order 2 (as the zero y-coordinate implies that the point is equal to its additive inverse) and so $18P = \mathcal{O}$. Since our calculations imply that no smaller multiple of P is equal to $\mathcal{O}$ in this group, we see that P is actually a generator of $(E_7, +) \cong \mathbb{Z}_{18}$.

Solution to Exercise 2.7

We follow the method outlined in Example 2.21. With the help of parts (a) and (b) of Lemma 2.10, Alice calculates

$$M_1 = kP = 5P = (1, -1) \quad \text{and}$$
$$M_2 = M + kP_B = (8, -3) + 5(-4, -4) = (0, 4),$$

and sends both ciphertexts M_1 and M_2 to Bob, who then calculates

$$M_2 - s_B M_1 = (0, 4) - 3(1, -1) = (8, -3),$$

which is Alice's original message.

With the extra knowledge of the solution to Exercise 2.6, however, one can avoid most of the applications of Lemma 2.10 and instead use the fact that the point $P = (0, 4)$ is a generator for the group $(E, +)$.

Solution to Exercise 2.8

We follow the method outlined in Example 2.22. Using parts (a) and (b) of Lemma 2.10, Alice computes $kP = 4(0, 4) = (8, -3)$ and $kP_B = 4(-4, -4) = (7, 3) = (d_1, d_2)$. She then determines $c_1 = d_1 m_1 = 14 \equiv -3 \pmod{17}$ and $c_2 = d_2 m_2 = 12 \equiv -5 \pmod{17}$. Therefore Alice's ciphertext is $(kP, c_1, c_2) = ((8, -3), -3, -5)$.

After receiving the ciphertext, Bob calculates $s_B(kP) = 3(8, -3) = (7, 3)$ and obtains $d_1 = 7$ and $d_2 = 3$. He then determines $d_1^{-1} = 5$ and $d_2^{-1} = 6$ in GF_{17}. Finally, he computes

$$c_1 d_1^{-1} = (-3) \times 5 \equiv 2 \pmod{17} \quad \text{and}$$
$$c_2 d_2^{-1} = (-5) \times 6 \equiv 4 \pmod{17},$$

thus recovering Alice's intended message $(2, 4)$.

We again point out that the extra knowledge of the solution to Exercise 2.6 allows one to avoid most of the applications of Lemma 2.10 by using the fact that the point $P = (0, 4)$ is a generator for the group $(E, +)$.

Index

adjoining a field element 95
algebraic element 91
algebraic extension 92, 93
algebraic over F 91
associativity
    in a vector space 87
automorphism 46
    of rings 46

basis
    in a vector space 89
Basis Theorem 90

canonical homomorphism 49
chain of ideals 26
characteristic of a field 82
ciphertext 188
closure
    in a vector space 87
commutativity
    in a vector space 87
constructible
    complex number 170
    point 159
    point in one move 159
    real number 163
    real number from a set S 163
content 15
coset 41
cryptosystem 187

degree 90
    of a field extension 90
derivation 123
Diffie–Hellman cryptosystem 209
Diffie–Hellman–ElGamal cryptosystem 234
discrete logarithm 211
discrete logarithm for elliptic curves 239
distributivity
    in a vector space 87
duplication of the cube 158, 168

$E_F(a, b)$ 215
elliptic curve 215
embeddings 76
evaluation homomorphism 51
extension of a field 85

$F(\alpha)$ 91
$F(s_1, \ldots, s_k)$ 142
F^* 107
Fast Euclidean Algorithm 190
Fermat numbers 195
field extension 85
field isomorphism 75
field of algebraic numbers in E over F 150
field of algebraic numbers over $\mathbb{Q}$ 150
field of fractions 12
field of Gaussian numbers 13
finite dimension 89
finitely generated ideal 37
First Isomorphism Theorem for rings 49
formal derivative 122
fraction in lowest terms 14

Galois field of p elements 84
general number sieve algorithm 205
GF_p 84, 188, 194

highest common factor 29
homomorphism property 11
    of a ring homomorphism 45
    of a ring isomorphism 11

ideal 21
    generated by an element 24
    maximal 52
    non-trivial 22
    prime 55
    proper 22
    square 39
identity
    in a vector space 87
Idiot's Binomial Theorem 84
image
    of a ring homomorphism 46
infinite dimension 89
int(x) 193
inverse
    in a vector space 87
isomorphic 75
isomorphism
    of fields 75
    of rings 11

kernel
    of a ring homomorphism 46
key exchange problem 187
KLM Theorem 103
kth root of unity 111

Laurent polynomials 19
line over F 221
line with slope 221
linear combination 89

linearly dependent 89
linearly independent 89
lowest common denominator 14

Menezes–Vanstone cryptosystem 237
minimal polynomial 96
morphism property 11
    of a ring homomorphism 45
    of a ring isomorphism 11

natural homomorphism 49

plaintext 188
point at infinity 215
points on an elliptic curve 215
prime field 83
prime ideal 55
primitive kth root of unity 111
primitive element 109
primitive polynomial 15
principal ideal 24
principal ideal domain 28
private key 188, 200
product of two ideals 36
proper ideal 22
public key 188, 200
public-key cryptosystems 188

$\overline{\mathbb{Q}}$ 150
quadratic residue of p 194
quadrature of the circle 158, 168, 169
quotient ring 42

Rabin–Miller test 207
ring homomorphism 45
ring isomorphism 11
root of unity 111
RSA cryptosystem 200
RSA triple 200

scalar multiplication 87
shared secret 209, 235
slopeless line 221
slopeless tangent line 222
span 89
spanning set 89
split 116
splitting field 115
splitting polynomial 116
square 194
square of an ideal 39
square root modulo p 194
squaring method 196
strong probable prime 207
subfield generated by a set 141
sum of two ideals 34
summary of results about integral domains 32

tangent line 222
tangent line with slope 222
transcendental 93
transcendental element 91
transcendental extension 92, 151
transcendental over F 91
trisection of an angle 158, 168, 169

vector addition 87
vector space 87

witness of non-primality 195, 207

zero
    in a vector space 87